CLAIMS

What is claimed is:

1. A computer-implemented method comprising:

providing a content resource by a content author for an access by a requester;

receiving, by the content author, a request, via a first channel, from the requester for accessing the content resource;

in response to the request, generating, by the content author, a session to access the content resource for the requester;

in response to the generated session, generating, by the content author, a payload identifying the content resource on a resource provider, wherein generating the payload further comprising embedding an embedded cryptographic content in the payload;

transmitting, by the content author, the generated payload to the requester;

receiving, by a resource provider, an authentication access request to the content resource, via a second channel, in response to executing, by the requester, the embedded cryptographic content, wherein the first channel and the second channel are different; and

in response to authenticating the authentication access request, providing, by the resource provider, the requester the access to the content resource.

2. The computer-implemented method of claim 1, wherein the session request comprises a server-to-server request call.

3. The computer-implemented method of claim 1, wherein the payload comprises a first data field identifying a location at the resource provider and a second data field for the cryptographic content.

4. The computer-implemented method of claim 1, wherein the content resource comprises computer software library executable files.

5. The computer-implemented method of claim 1, wherein the session comprises a timed application stack or a web token.

6. The computer-implemented method of claim 1, wherein the location comprises a uniform resource locator (URL) or a uniform resource identifier (URI).

7. The computer-implemented method of claim 1, wherein the second channel comprises a subresource integrity (SRI) via a web browser.

8. A computer-implemented method comprising:

receiving, by a content author, a request, via a first channel, from a requester for accessing a content resource;

in response to the request, generating, by the content author, a session to access the content resource for the requester;

in response to the generated session, generating, by the content author, a payload identifying the content resource on a resource provider, wherein generating the payload further comprising embedding an embedded cryptographic content in the payload;

transmitting, by the content author, the generated payload to the requester;

receiving, by a resource provider, an authentication access request to the content resource, via a second channel, in response to executing, by the requester, the embedded cryptographic content, wherein the first channel and the second channel are different; and

in response to authenticating the authentication access request, providing, by the resource provider, the requester the access to the content resource.

9. The computer-implemented method of claim 8, wherein the session request comprises a server-to-server request call.

10. The computer-implemented method of claim 8, wherein the payload comprises a first data field identifying a location at the resource provider and a second data field for the cryptographic content.

11. The computer-implemented method of claim 8, wherein the content resource comprises computer software library executable files.

12. The computer-implemented method of claim 8, wherein the session comprises a timed application stack or a web token.

13. The computer-implemented method of claim 8, wherein the location comprises a uniform resource locator (URL) or a uniform resource identifier (URI).

14. The computer-implemented method of claim 8, wherein the second channel comprises a subresource integrity (SRI) via a web browser.

15. A system comprising:

a content server configured to receive a request, via a first channel, from a requester for accessing a content resource;

in response to the request, the content server is configured to generate a session to access the content resource for the requester;

in response to the generated session, the content server is configured to generate a payload identifying the content resource on a resource server;

wherein the content server is configured to transmit the generated payload to the requester;

wherein the resource server is configured to receive an authentication access request, via a second channel, in response to executing, by the requestor, the embedded cryptographic content, wherein the first channel and the second channel are different; and

in response to authenticating the authentication access request, the resource server is configured to provide the requester the access to the content resource.

16. The system of claim 15, wherein the session request comprises a server-to-server request call.

17. The system of claim 15, wherein the payload comprises a first data field identifying a location at the resource provider and a second data field for the cryptographic content.

18. The system of claim 15, wherein the session comprises a timed application stack or a web token.

19. The system of claim 15, wherein the location comprises a uniform resource locator (URL) or a uniform resource identifier (URI).

20. The system of claim 15, wherein the second channel comprises a subresource integrity (SRI) via a web browser.