CLAIM

1. A method, comprising:

receiving, by a tokenization hub server comprising a token request interface, a token type module configured to identify a type of token requested based on a device type, and a token provisioning module, a first token request from a first application on a first mobile device via the token request interface, the first mobile device comprising a secure element and the first token request comprising a first device type identifier;

determining, by the tokenization hub server, based on the first device type identifier in the first token request, first mobile device information comprising information indicating that the first mobile device has the secure element;

determining, by the token type module in the tokenization hub server, a static token corresponding to the first mobile device information;

sending, by the tokenization hub server, a first request for the static token to a CTC module;

receiving, by the tokenization hub server, the static token from the CTC module;

returning, by the token provisioning module in the tokenization hub server, the static token to the first mobile device;

writing the static token to the secure element in the first mobile device;

receiving, by the token request interface in the tokenization hub server, a second token request from a second application on a second mobile device comprising a non-secure element, the second token request comprising a second device type identifier;

determining, by the tokenization hub server, based on the second device type identifier in the second token request, second mobile device information comprising information indicating that the second mobile device does not have a secure element;

determining, by the token type module in the tokenization hub server, a dynamic token corresponding to the second mobile device information and a time to live value associated with the dynamic token;

storing, by the tokenization hub server, the time to live value associated with the dynamic token;

sending, by the tokenization hub server, a second request for the dynamic token to the CTC module;

receiving, by the tokenization hub server, the dynamic token from the CTC module;

returning, by the token provisioning module in the tokenization hub server, the dynamic token to the second application on the second mobile device; and

storing the dynamic token in the non-secure element in the second mobile device.

2. The method of claim 1, wherein returning the static token to the first mobile device further comprises:

sending the static token to a provisioning service, wherein the provisioning service opens a secure connection to the first mobile device.

3. The method of claim 1, further comprising:

persisting, by the tokenization hub server, the first mobile device information in a credential database in a payment processing network.

4. A system comprising:

a mobile tokenization hub server computer comprising a processor and a non-transitory computer readable storage medium including instructions stored thereon which, when executed by the processor cause the processor to implement a method of:

receiving a first token request from a first application on a first mobile device via a token request interface, the first mobile device comprising a secure element and the first token request comprising a first device type identifier;

determining based on the first device type identifier in the first token request, first mobile device information comprising

information indicating that the first mobile device has the secure element;

determining, by a token type module, a static token corresponding to the first mobile device information;

sending a first request for the static token to a CTC module configured to communicate with the mobile tokenization hub server computer;

receiving a first static token from the CTC module;

returning, by a token provisioning module, the first token to the first mobile device;

receiving, by the token request interface, a second token request from a second application on a second mobile device comprising a non-secure element, the second token request comprising a second device type identifier;

determining based on the second device type identifier in the second token request, second mobile device information comprising information indicating that the second mobile device does not have a secure element;

determining, by the token type module, a dynamic token corresponding to the second mobile device information and a time to live value associated with the dynamic token;

storing the time to live value associated with the dynamic token;

sending a second request for the dynamic token to the CTC module;

receiving the dynamic token from the CTC module; and

returning, by the token provisioning module, the dynamic token to the second application on the second mobile device.

5. The system of claim 4, wherein returning the static token to the first mobile device further comprises:

sending the static token to a provisioning service, wherein the provisioning service opens a secure connection to the first mobile device.

6. The method of claim 4, wherein the method further comprises:

persisting the first and second mobile device information in a credential database in a payment processing network.