Digital Coins in Swaptacular

Evgeni Pandurksi

2022-09-10

Overview

This document specifies the way *digital coins* work in Swaptacular.

In Swaptacular's terminology, the word "debtor" means a Swaptacular currency, with its respective issuer. A "digital coin" is a specially formatted URL, which uniquely identifies a debtor (a currency) in Swaptacular, and contains a reference to a document that describes the currency.

Note: The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Digital Coin

The general form of a *digital coin* is:

`<debtor-info-locator>#<swpt-debtor-uri>`

- `<debtor-info-locator>` is the Debtor Info Locator (see below).
- `<swpt-debtor-uri>` is an URI in the `swpt` URI scheme[1], which uniquely identifies the debtor.

Example: `https://example.com/foo/bar#swpt:6787514562`

Here the URL `https://example.com/foo/bar` is the Debtor Info Locator, and `swpt:6787514562` is the URI that uniquely identifies the debtor.

Note: The preferred way to make digital coins available to currency users is to present them as QR Codes, whose textual content consists of the respective digital coin. For the example given above, the textual context of the corresponding QR Code will be: `https://example.com/foo/bar#swpt:6787514562`.

[1] The `swpt` URI scheme is defined in a separate document.

Debtor Info Locator

"Debtor Info Locator" is an HTTPS URL, making a network request to which, MUST either directly return[2] an *immutable document* that describes the currency, or redirects[3] to a different URL, from which an *immutable document* that describes the currency can be retrieved. The retrieved document MUST be immutable. [4]

Important note: When the description of the currency changes, a new immutable document (with a new URL) MUST be created, containing the new description, and the currency's "Debtor Info Locator" MUST be updated to redirect to the newly created (the latest) version of the currency description document.

Debtor Info Documents

In Swaptacular, a machine-readable document that describes a currency is called a "Debtor Info Document". A multitude of standard formats can be used for debtor info documents, which shall be defined in their respective format specifications.

As an absolute minimum, every debtor info document MUST contain:

- the currency's Debtor Info Locator,
- the `swpt`[5] URI which uniquely identifies the debtor,
- the currency name.

Furthermore, debtor info documents SHOULD contain additional essential information about the respective currency: the currency's display parameters (like the currency unit abbreviation), the currency description, optional fixed exchange rate with another currency, etc.

Verification of Digital Coins

Debtor info documents SHOULD always be retrieved via cryptographically secured connections, HTTPS for example. Although HTTPS (which is REQUIRED for Debtor Info Locators) gives a good level of security, the information contained in a debtor info document is of such critical importance, that its authenticity SHOULD be independently verified before the user is allowed to receive payments in the corresponding currency. The following verification procedure SHOULD be followed:

1. If the user does not have an account with the debtor specified by `<swpt-debtor-uri>` already, the user's *creditors agent* should send a

[2] That is: Directly return an HTTP response, with response code `200`, that contains an immutable document which describes the currency.

[3] The redirection SHOULD use HTTP response code `302`.

[4] In this context, "immutable" means that later requests to the same URL, MUST return exactly the same document.

[5] The `swpt` URI scheme is defined in a separate document.

`ConfigureAccount` Swaptacular Messaging Protocol message to the *accounting authority* responsible for the given debtor. This message instructs the accounting authority to create a new account with the given debtor.

2. If a new account with the given debtor **can not** be created, the verification attempt has failed, and the user will not be able to receive payments in the corresponding currency.[6]

   Note however, that in this case, a "dummy" account with the given debtor can still be created for the user. Such a dummy account can only be used as a peg for currencies that have declared a fixed exchange rate with the given currency.

3. If an account with the given debtor has been successfully created, the user's *creditors agent* will receive an `AccountUpdate` Swaptacular Messaging Protocol message from the *accounting authority* responsible for the debtor. The received message will contain the following fields: `debtor_info_iri`, `debtor_info_content_type`, and `debtor_info_sha256`.

4. If the values received in the previous step (that is: `debtor_info_iri`, `debtor_info_content_type`, and `debtor_info_sha256`) confirm the information obtained directly from the digital coin, then the digital coin has been successfully verified, and the user may be allowed to receive payments in the corresponding currency.

[6] When a permanent network connection is not configured between the user's *creditors agent* and *accounting authority* responsible for the given debtor, the attempt to create a new account will fail. Note that this scenario is not uncommon, and should be expected.