Signed e-Receipts – Invention Disclosure

This document is based on the e-receipt distribution model outlined in:
https://cyberphone.github.io/doc/defensive-publications/e-receipts.pdf

Problem Definition

How do you verify the signature of an e-receipt in a world with millions of merchants?

Imagine the following payment request taken from the mentioned e-receipt document:
Space Shop is obviously the issuer of the e-receipt.

```
{
  "paymentRequest": {
    "commonName": "Space Shop",
    "amount": "550.00",
    "currency": "EUR",
    "referenceId": "20231007
  },
  "receiptUrl": "https://spaceshop.com/receipts/20231007j5lOEL2w9cWBFUwkbrFgjQ"
}
```

Non-normative sample request

On the next page you will find a verifiable e-receipt...

e-Receipt creation:

Prerequisite: The Merchant has an already created key-pair where the public key is published at "validationKeyUrl”

- The Merchant signs a newly created e-receipt using the private key
- The Merchant publishes the signed e-receipt at "receiptUrl"

```
{
  "receiptUrl": "https://spaceshop.com/receipts/20231007j5lOEL2w9cWBFUwkbrFgjQ",
  "validationKeyUrl": "https://spaceshop.com/keys/ed25519-1.jwk",
  "receipt": {
    "description": "A bunch of stuff",
    "amount": "550.00",
    "currency": "EUR"
  },
  "signature": {
    "algorithm": "Ed25519",
    "publicKey": {
      "kty": "OKP",
      "crv": "Ed25519",
      "x": "_kms9bkrbpI1lPLoM2j2gKySS-k89TOuyvgC43dX-Mk"
    },
    "value": "Ap-Rc7GSGPHhnq7….PyiHT-PeIpzgdjsrE2fOjTuAQ"
  }
}
```

Non-normative sample e-receipt data

Non-normative JSON signature solution
https://cyberphone.github.io/doc/security/jsf.html

e-Receipt Validation steps:

- Verify that "receiptUrl" is identical to the URL used for fetching the e-receipt
- Verify that the "validationKeyUrl” has the same host-name as "receiptUrl"
- Verify that the signature validates using the "publicKey” of the "signature
- Fetch the key published at "validationKeyUrl” using an HTTP GET and verify that the received key is identical to the "publicKey” of the "signature

If all steps succeed, the e-receipt is authentic with respect to the domain spaceshop.com.

Note: although the sample uses JSON, the same concept can be applied to any format and signature.