

# Payment Method Manifest

Max Alibaba  
Zkoch Google

# Use Cases

- The ability to confirm the authenticity of payment apps associated with payment methods. If a user installs a payment application associated with a proprietary payment method on their platform of choice, we want to verify that the app is who it claims to be.
- The ability for proprietary payment methods to control what other payment apps in the system are able to support their payment method.
- The ability for payment mediators to offer improved UX in cases where a users wants to use a payment method but doesn't have a necessary app installed (i.e. run-time or dynamic payment app registration/installation).

RFC5988: HTTP Link Header

Link: </bobpay/pay/payment-manifest.json>; rel="payment-method-manifest"



Browser

bobpay  
Website

## webappmanifest.json

```
{
  "name": "BobPay - World's Greatest Payment Method",
  "description": "This payment method changes lives",
  "short_name": "BobPay",
  "icons": [{
    "src": "icon/lowres.webp",
    "sizes": "64x64",
    "type": "image/webp"
  }, {
    "src": "icon/lowres.png",
    "sizes": "64x64"
  }, {
    "src": "icon/hd_hi",
    "sizes": "128x128"
  }],
  "serviceworker": {
    "src": "payment-sw.js",
    "scope": "/pay",
    "use_cache": false
  }
  "related_applications": [
    {
      "platform": "play",
      "url": "https://play.google.com/store/apps/details?id=com.bobpay",
      "sha256_cert_fingerprints": ["59:5C:88:65:FF:C4:E8:20:CF:F7:3E:C8..."], //new
      "version": 1, // new
      "id": "com.example.app1"
    }, {
      "platform": "itunes",
      "url": "https://itunes.apple.com/app/example-app1/id123456789",
    }
  ]
}
```

# Anticipated FAQ

- Q1: Why such heavy reliance on web app manifests?
  - A: They already have almost all the data we need (icons, labels, service workers, related\_applications), so it didn't seem to make sense to try and duplicate this information inside of the payment method manifest.
  - It also allows us to cleanly separate the idea of "payment method" and "payment app". Payment methods always have a payment method manifest and payment apps always have a web app manifest. So clean. Amaze.

- Q2: Isn't there a security concern with run-time installation of payment apps?
  - A: The risk is not greater than what's already present on the web. Origin is still going to play a big role in helping users determine what to install, and user agents will continue to invest in blocking nefarious actors.

- Q3: I don't understand what supported\_origins is for. Help?
  - In most cases today, there is a 1:1 correspondance between proprietary payment method and supported payment app. PayPal is a good example. If a merchant supports PayPal payments, only PayPal can successfully authorize that transaction (right now).
  - But this isn't always the case. Let's take a made up example. We have the greatest payment method in the world, BobPay, with an identifying URL of "https://bobpay.xyz/pay". We then have a Payment App called "Alice Pay" (located at https://alicepay.xyz), which is a really popular P2P payment app. BobPay and AlicePay make a deal that says wherever BobPay is accepted, users can use their AlicePay application to pay. GeorgePay, however, a competing P2P payment app has not entered into the same agreement, so unfortunatly GeorgePay cannot be used to pay when a merchant accepts BobPay.
  - We need some way for BobPay to easily express this relationship structure. This is what "supported\_origins" is for. By putting "https://alicepay.xyz" as a supported origin, if the user agent ever encounters a Payment App for AlicePay claiming support for BobPay, we can verify that with BobPay.

- Q4: Why supported origins and not supported absolute URLs? Or why not link to the supported web app manifest directly?
- A: This would just make a much tighter coupling between entities than what is necessary. In the case of the above BobPay and AlicePay scenario, AlicePay has to keep BobPay informed any time their payment app location changes. This is incredibly difficult to scale. Our primary purpose is validating the relationship, nothing more.