Pwning Apple Wallet ecosystem and its apps

The Hidden Dangers Lurking in Your Pocket

Priyank Nigam

Microsoft Red Team

Bio

- Senior **Red** Teamer @Microsoft
- Bug Bounties/Responsible Disclosures
- Research Interests
  - AppSec (Web/mobile/AI/LLMs)
  - IoT
  - Network Sec
  - MS Azure

- ~~Senior~~ **Blue** Teamer @Home
  - My toddler (+ infant) -> Learn from folks who know no “rules” -> Just like real-world Threat actors! ☺

Agenda

- Attack Wallet App
- Attack all apps which support adding passes to wallet

- Fun!

DISCLAIMER: All material is for research and educational purposes only. Any actions and or activities related to the material contained within this talk is solely your responsibility. The authors will not be held responsible in the event any criminal charges resulting from the misuse of this information and for breaking of federal and local laws.

What is a Wallet Pass?

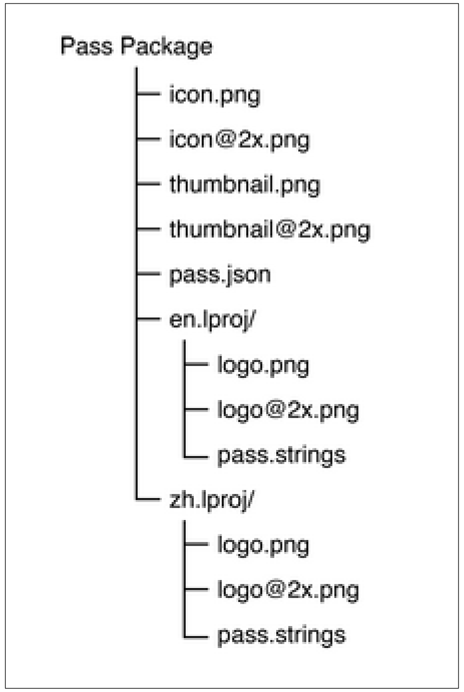
Add to
Apple Wallet

- Passes are a digital representation of information that might otherwise be printed on small pieces of paper or plastic.
- They let users take an action in the physical world.
- Passes can contain images and a barcode, and you can update passes using push notifications.
- The pass library contains the user’s passes, and users view and manage their passes using the Wallet app

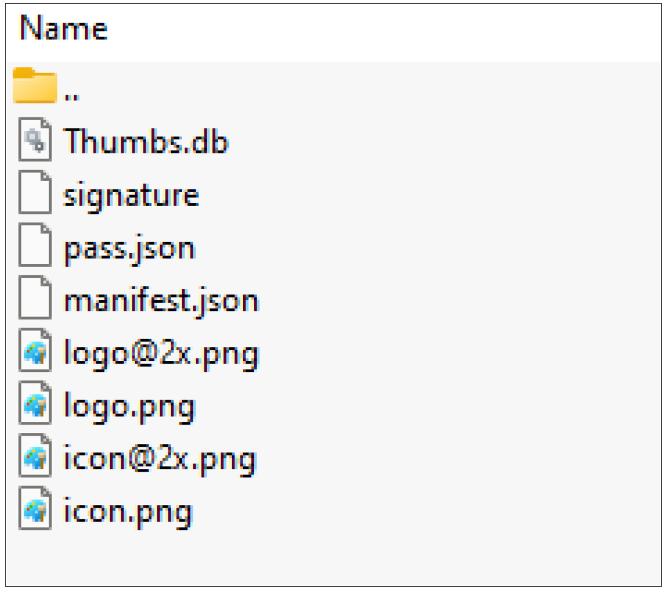
What’s inside it?

- Passes are created as a package (also referred to as a bundle) containing a `pass.json` file that defines the pass, and image assets such as the logo and the icon.

  Every pass has a pass type identifier associated with a developer account.



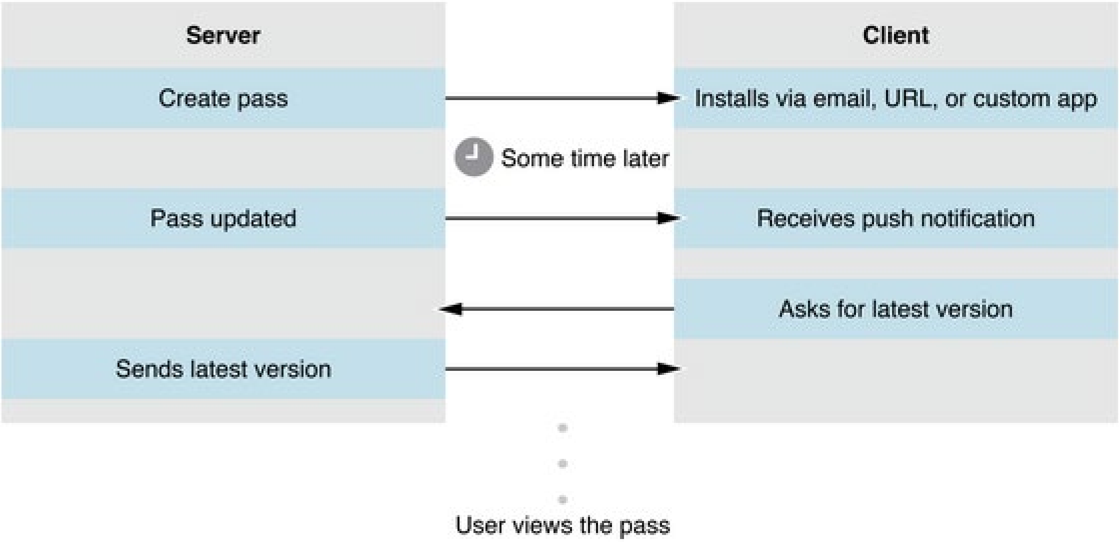
```
Pass Package
    ├─ icon.png
    ├─ icon@2x.png
    ├─ thumbnail.png
    ├─ thumbnail@2x.png
    ├─ pass.json
    ├─ en.lproj/
    │    ├─ logo.png
    │    ├─ logo@2x.png
    │    └─ pass.strings
    └─ zh.lproj/
         ├─ logo.png
         ├─ logo@2x.png
         └─ pass.strings
```



```
Name
..
Thumbs.db
signature
pass.json
manifest.json
logo@2x.png
logo.png
icon@2x.png
icon.png
```

How does it work?

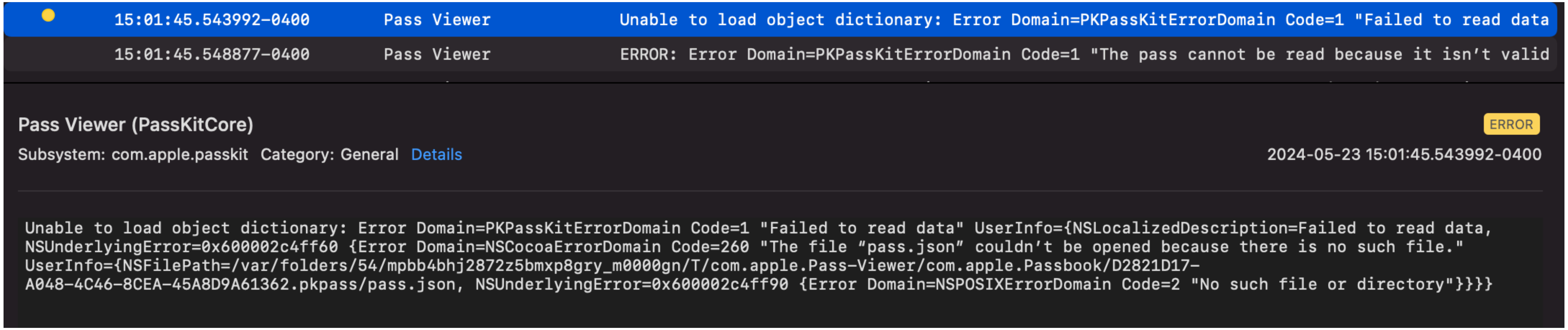
- User is redirected to an online service which hosts the Pass
- They install it via the default Wallet app on iOS
- They present it whenever they need to utilize a service



- They live happily ever after

How does it ACTUALLY work?

If .pkpass is not well formed



```
15:01:45.543992-0400    Pass Viewer    Unable to load object dictionary: Error Domain=PKPassKitErrorDomain Code=1 "Failed to read data
15:01:45.548877-0400    Pass Viewer    ERROR: Error Domain=PKPassKitErrorDomain Code=1 "The pass cannot be read because it isn’t valid
```

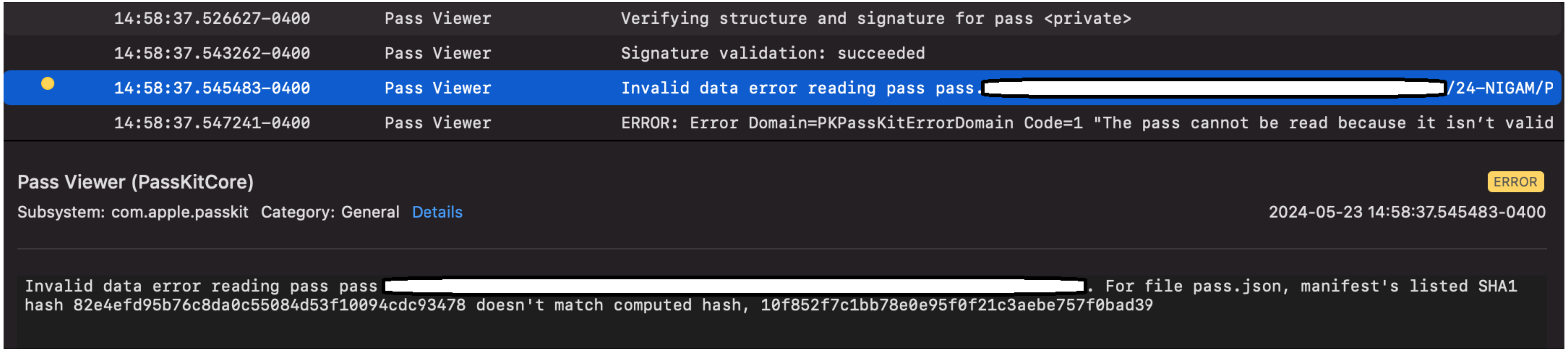
Pass Viewer (PassKitCore)

Subsystem: com.apple.passkit Category: General Details

2024-05-23 15:01:45.543992-0400

```
Unable to load object dictionary: Error Domain=PKPassKitErrorDomain Code=1 "Failed to read data" UserInfo={NSLocalizedDescription=Failed to read data,
NSUnderlyingError=0x600002c4ff60 {Error Domain=NSCocoaErrorDomain Code=260 "The file “pass.json” couldn’t be opened because there is no such file."
UserInfo={NSFilePath=/var/folders/54/mpbb4bhj2872z5bmxp8gry_m0000gn/T/com.apple.Pass-Viewer/com.apple.Passbook/D2821D17-
A048-4C46-8CEA-45A8D9A61362.pkpass/pass.json, NSUnderlyingError=0x600002c4ff90 {Error Domain=NSPOSIXErrorDomain Code=2 "No such file or directory"}}}}
```

If any file is tampered



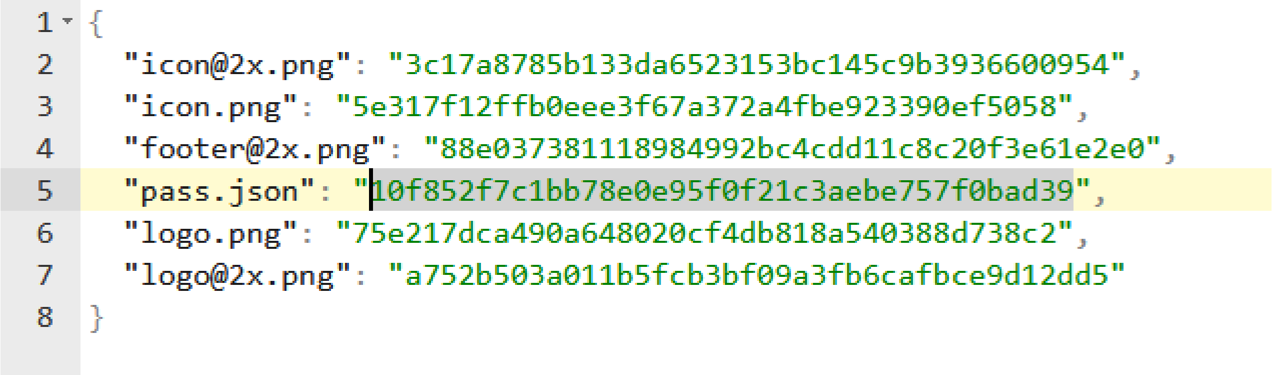
```
14:58:37.526627-0400    Pass Viewer    Verifying structure and signature for pass <private>
14:58:37.543262-0400    Pass Viewer    Signature validation: succeeded
14:58:37.545483-0400    Pass Viewer    Invalid data error reading pass pass.[redacted]/24-NIGAM/P
14:58:37.547241-0400    Pass Viewer    ERROR: Error Domain=PKPassKitErrorDomain Code=1 "The pass cannot be read because it isn't valid
```

Pass Viewer (PassKitCore) ERROR

Subsystem: com.apple.passkit Category: General Details 2024-05-23 14:58:37.545483-0400

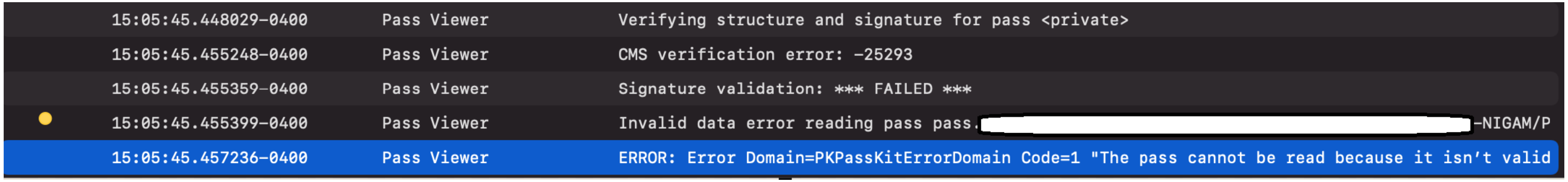
```
Invalid data error reading pass pass[redacted]. For file pass.json, manifest's listed SHA1
hash 82e4efd95b76c8da0c55084d53f10094cdc93478 doesn't match computed hash, 10f852f7c1bb78e0e95f0f21c3aebe757f0bad39
```

Tamper the manifest?

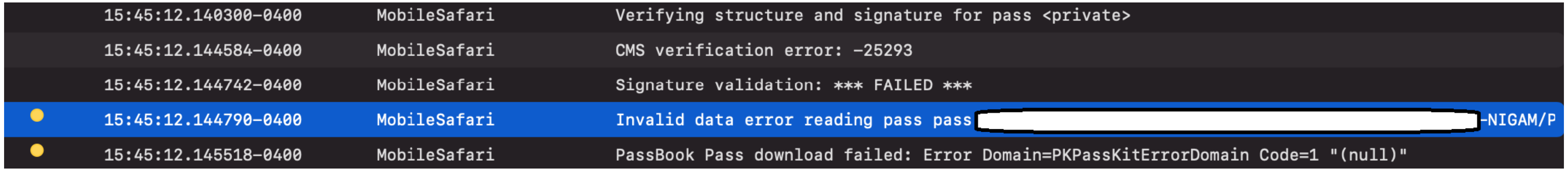


```
{
  "icon@2x.png": "3c17a8785b133da6523153bc145c9b3936600954",
  "icon.png": "5e317f12ffb0eee3f67a372a4fbe923390ef5058",
  "footer@2x.png": "88e037381118984992bc4cdd11c8c20f3e61e2e0",
  "pass.json": "10f852f7c1bb78e0e95f0f21c3aebe757f0bad39",
  "logo.png": "75e217dca490a648020cf4db818a540388d738c2",
  "logo@2x.png": "a752b503a011b5fcb3bf09a3fb6cafbce9d12dd5"
}
```

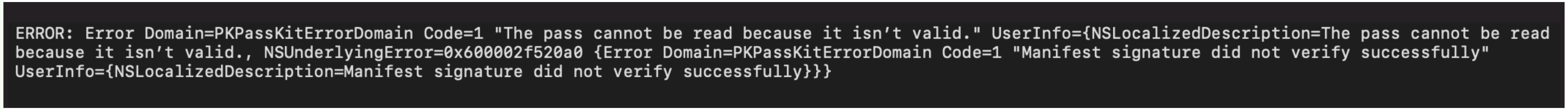
If the hash itself is tampered



```
      15:05:45.448029-0400    Pass Viewer    Verifying structure and signature for pass <private>
      15:05:45.455248-0400    Pass Viewer    CMS verification error: -25293
      15:05:45.455359-0400    Pass Viewer    Signature validation: *** FAILED ***
●     15:05:45.455399-0400    Pass Viewer    Invalid data error reading pass pass.[redacted]-NIGAM/P
      15:05:45.457236-0400    Pass Viewer    ERROR: Error Domain=PKPassKitErrorDomain Code=1 "The pass cannot be read because it isn't valid
```



```
      15:45:12.140300-0400    MobileSafari    Verifying structure and signature for pass <private>
      15:45:12.144584-0400    MobileSafari    CMS verification error: -25293
      15:45:12.144742-0400    MobileSafari    Signature validation: *** FAILED ***
●     15:45:12.144790-0400    MobileSafari    Invalid data error reading pass pass[redacted]-NIGAM/P
●     15:45:12.145518-0400    MobileSafari    PassBook Pass download failed: Error Domain=PKPassKitErrorDomain Code=1 "(null)"
```



```
ERROR: Error Domain=PKPassKitErrorDomain Code=1 "The pass cannot be read because it isn't valid." UserInfo={NSLocalizedDescription=The pass cannot be read
because it isn't valid., NSUnderlyingError=0x600002f520a0 {Error Domain=PKPassKitErrorDomain Code=1 "Manifest signature did not verify successfully"
UserInfo={NSLocalizedDescription=Manifest signature did not verify successfully}}}
```

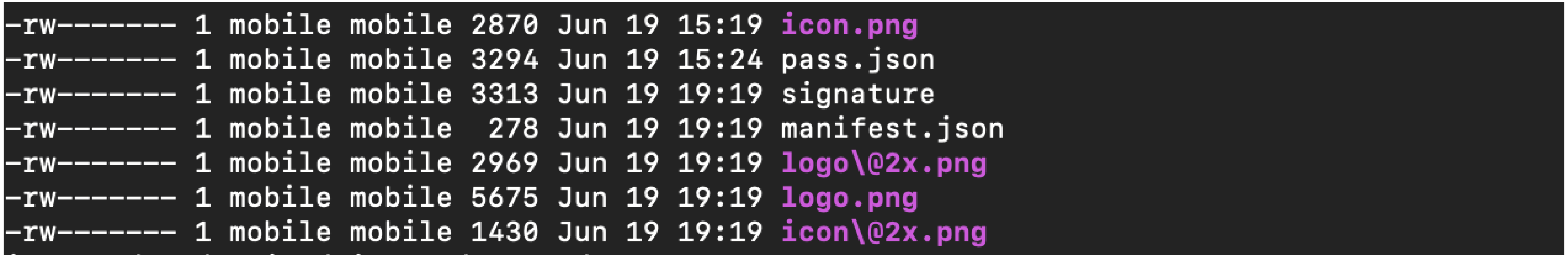
So tampered passes cannot be installed

But what happens AFTER the install?

Install Location

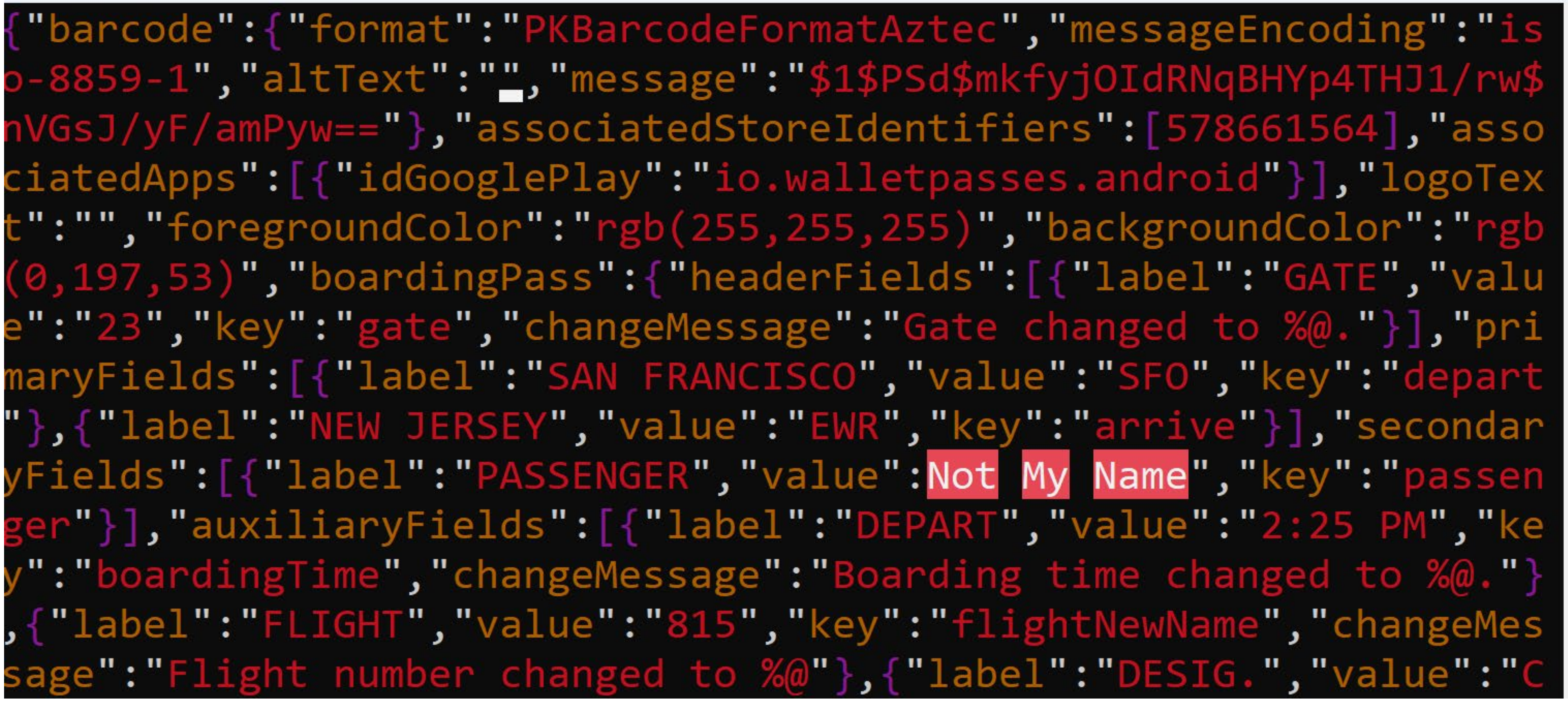
```
drwxr-xr-x  5 mobile mobile 160 Jun 19 15:19 hgxbqyagOuCYFZLl5B3Uk4keKhg\=.cache/
drwx------ 10 mobile mobile 320 Jun 19 15:23 g+1NKwFUhhlz-QLoATzxtpnCXM0\=.pkpass/
drwx------  9 mobile mobile 288 Jun 19 17:34 hgxbqyagOuCYFZLl5B3Uk4keKhg\=.pkpass/
```

All same files!



```
-rw------- 1 mobile mobile 2870 Jun 19 15:19 icon.png
-rw------- 1 mobile mobile 3294 Jun 19 15:24 pass.json
-rw------- 1 mobile mobile 3313 Jun 19 19:19 signature
-rw------- 1 mobile mobile  278 Jun 19 19:19 manifest.json
-rw------- 1 mobile mobile 2969 Jun 19 19:19 logo\@2x.png
-rw------- 1 mobile mobile 5675 Jun 19 19:19 logo.png
-rw------- 1 mobile mobile 1430 Jun 19 19:19 icon\@2x.png
```

Let’s edit and reload?



```
{"barcode":{"format":"PKBarcodeFormatAztec","messageEncoding":"is
o-8859-1","altText":"","message":"$1$PSd$mkfyjOIdRNqBHYp4THJ1/rw$
nVGsJ/yF/amPyw=="},"associatedStoreIdentifiers":[578661564],"asso
ciatedApps":[{"idGooglePlay":"io.walletpasses.android"}],"logoTex
t":"","foregroundColor":"rgb(255,255,255)","backgroundColor":"rgb
(0,197,53)","boardingPass":{"headerFields":[{"label":"GATE","valu
e":"23","key":"gate","changeMessage":"Gate changed to %@."}],"pri
maryFields":[{"label":"SAN FRANCISCO","value":"SFO","key":"depart
"},{"label":"NEW JERSEY","value":"EWR","key":"arrive"}],"secondar
yFields":[{"label":"PASSENGER","value":Not My Name","key":"passen
ger"}],"auxiliaryFields":[{"label":"DEPART","value":"2:25 PM","ke
y":"boardingTime","changeMessage":"Boarding time changed to %@."}
,{"label":"FLIGHT","value":"815","key":"flightNewName","changeMes
sage":"Flight number changed to %@"},{"label":"DESIG.","value":"C
```

```
{
"description" : "Boarding pass for October 4, San Francisco to
London",
"formatVersion" : 1,
"passTypeIdentifier" : "pass.com.example.boarding-pass",
"serialNumber" : "123456",
"boardingPass" : {
"primaryFields
"label" : "San Francisco",
"value" : "SFO"
ds" : [
{
"key" : "origin",},
{
"key" : "destination",
"label" : "London",
"value" : "LHR"
}],
"secondaryFields" : [{
"key" : "boarding-gate",
"label" : "Gate",
"value" : "F12"
}],
"auxiliaryFields" : [{
"key" : "seat",
"label" : "Seat",
"value" : "7A"
},
{
"key" : "passenger-name",
"label" : "Passenger",
"value" : "John Appleseed"
}],
"transitType" : "PKTransitTypeAir"
} }
```

Which files/fields can be tampered?

Impact

Loyalty and rewards cards

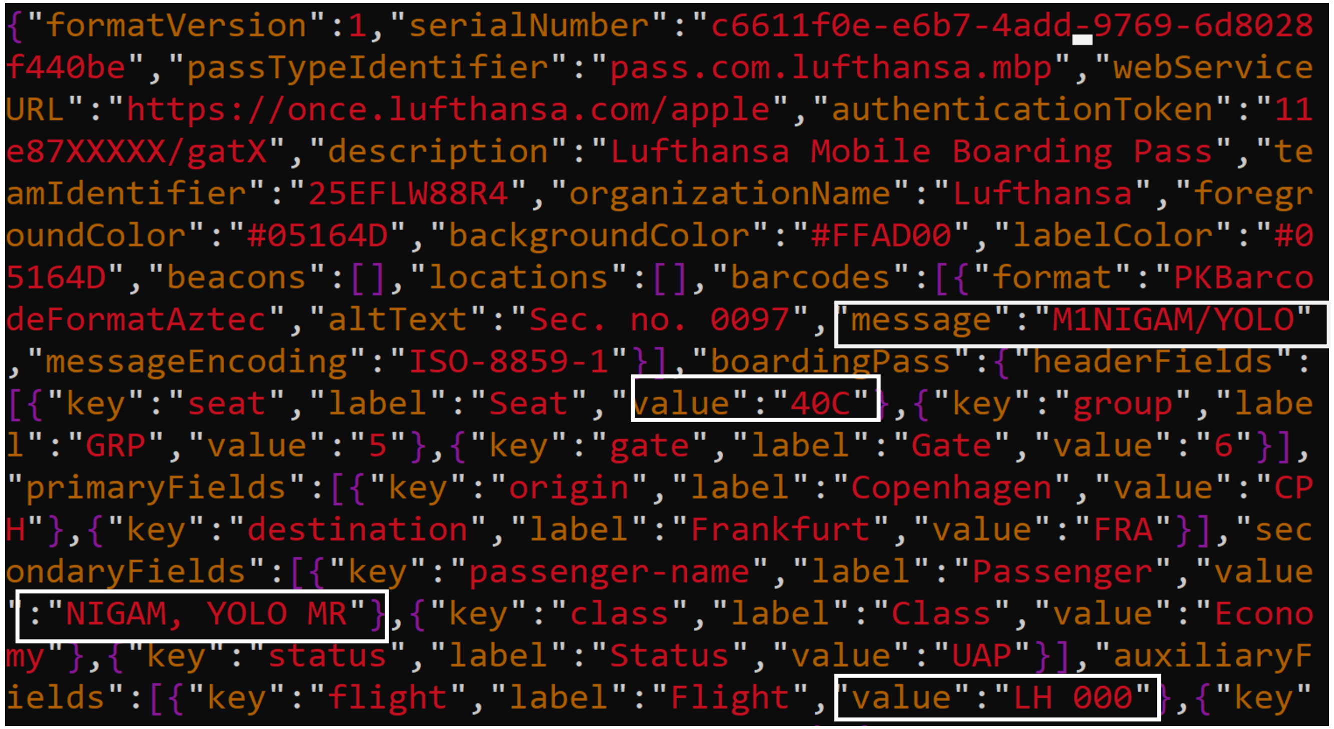
Coupons

Boarding Passes

Movie/Event Tickets

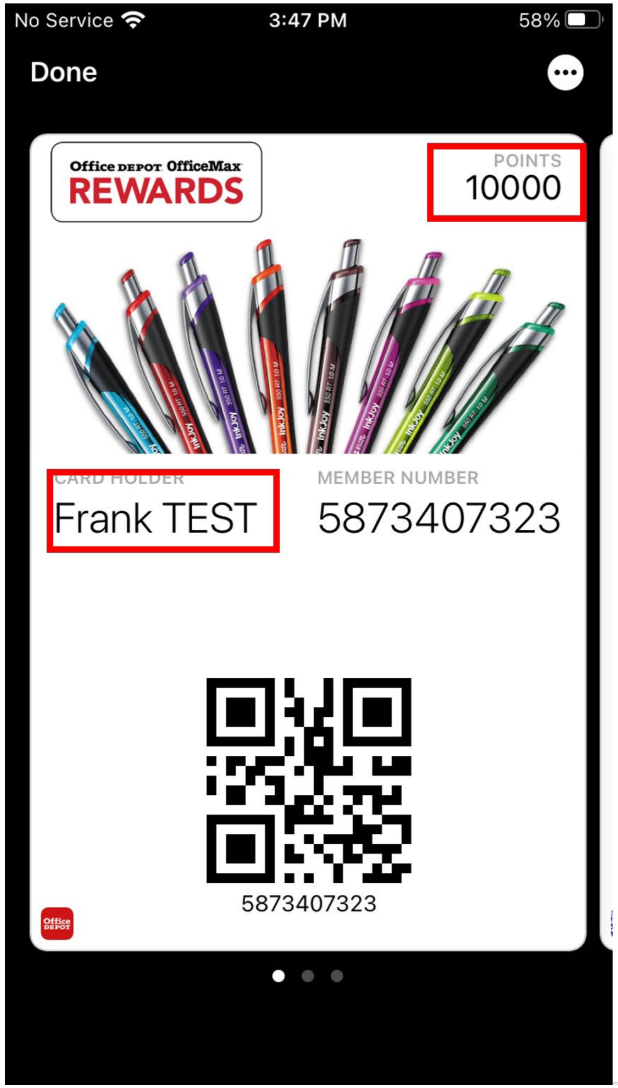
** Apple Pay Not Affected*

(Live?) Demo



```
{"formatVersion":1,"serialNumber":"c6611f0e-e6b7-4add-9769-6d8028
f440be","passTypeIdentifier":"pass.com.lufthansa.mbp","webService
URL":"https://once.lufthansa.com/apple","authenticationToken":"11
e87XXXXX/gatX","description":"Lufthansa Mobile Boarding Pass","te
amIdentifier":"25EFLW88R4","organizationName":"Lufthansa","foregr
oundColor":"#05164D","backgroundColor":"#FFAD00","labelColor":"#0
5164D","beacons":[],"locations":[],"barcodes":[{"format":"PKBarco
deFormatAztec","altText":"Sec. no. 0097","message":"M1NIGAM/YOLO"
,"messageEncoding":"ISO-8859-1"}],"boardingPass":{"headerFields":
[{"key":"seat","label":"Seat","value":"40C"},{"key":"group","labe
l":"GRP","value":"5"},{"key":"gate","label":"Gate","value":"6"}],
"primaryFields":[{"key":"origin","label":"Copenhagen","value":"CP
H"},{"key":"destination","label":"Frankfurt","value":"FRA"}],"sec
ondaryFields":[{"key":"passenger-name","label":"Passenger","value
":"NIGAM, YOLO MR"},{"key":"class","label":"Class","value":"Econo
my"},{"key":"status","label":"Status","value":"UAP"}],"auxiliaryF
ields":[{"key":"flight","label":"Flight","value":"LH 000"},{"key"
```

Impact



No Service 3:47 PM 58%

Done

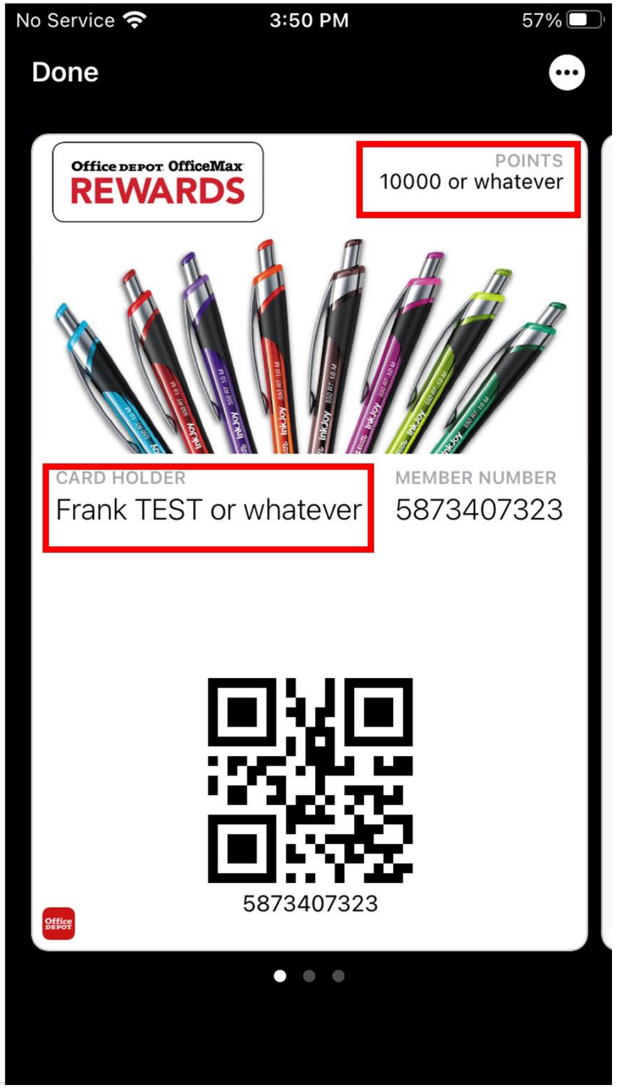
Office DEPOT OfficeMax REWARDS

POINTS
10000

CARD HOLDER
Frank TEST

MEMBER NUMBER
5873407323

5873407323



No Service 3:50 PM 57%

Done

Office DEPOT OfficeMax REWARDS

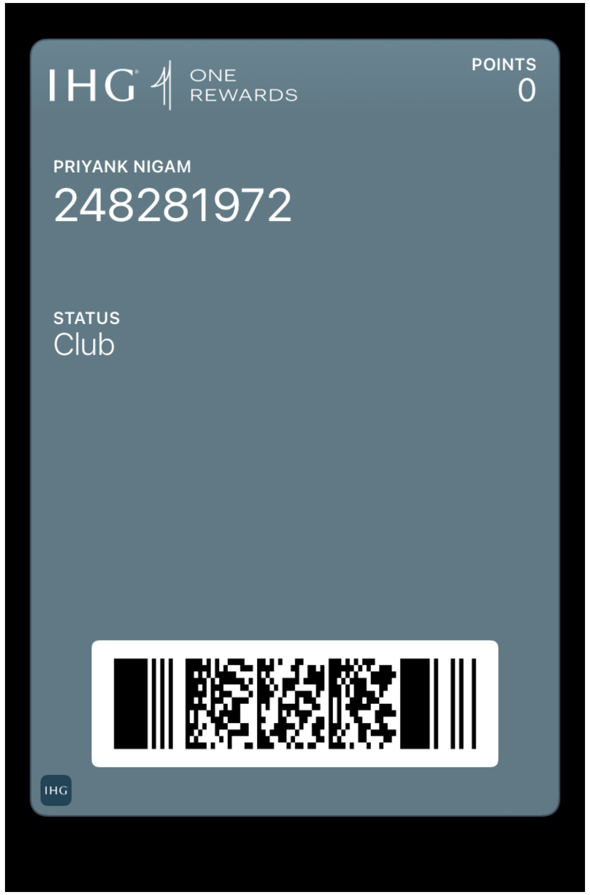
POINTS
10000 or whatever

CARD HOLDER
Frank TEST or whatever

MEMBER NUMBER
5873407323

5873407323

Impact?

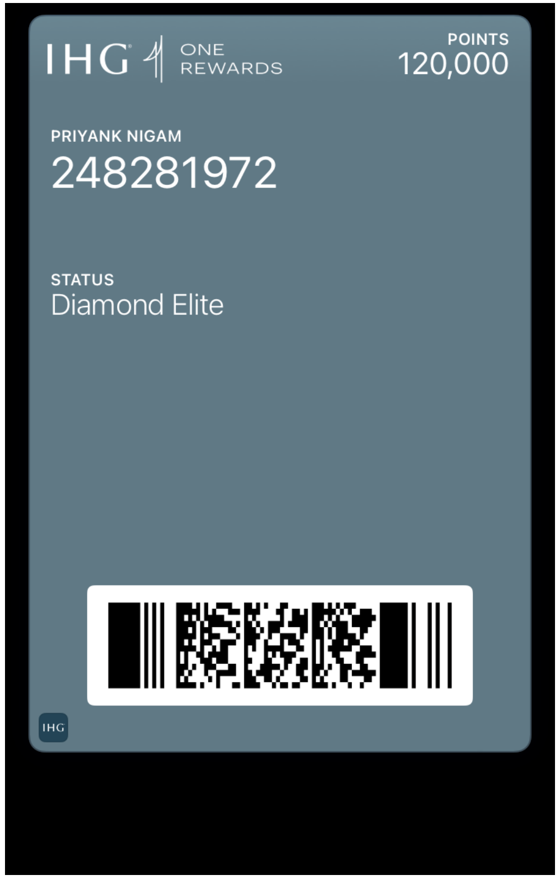


IHG ONE REWARDS

POINTS
0

PRIYANK NIGAM
248281972

STATUS
Club



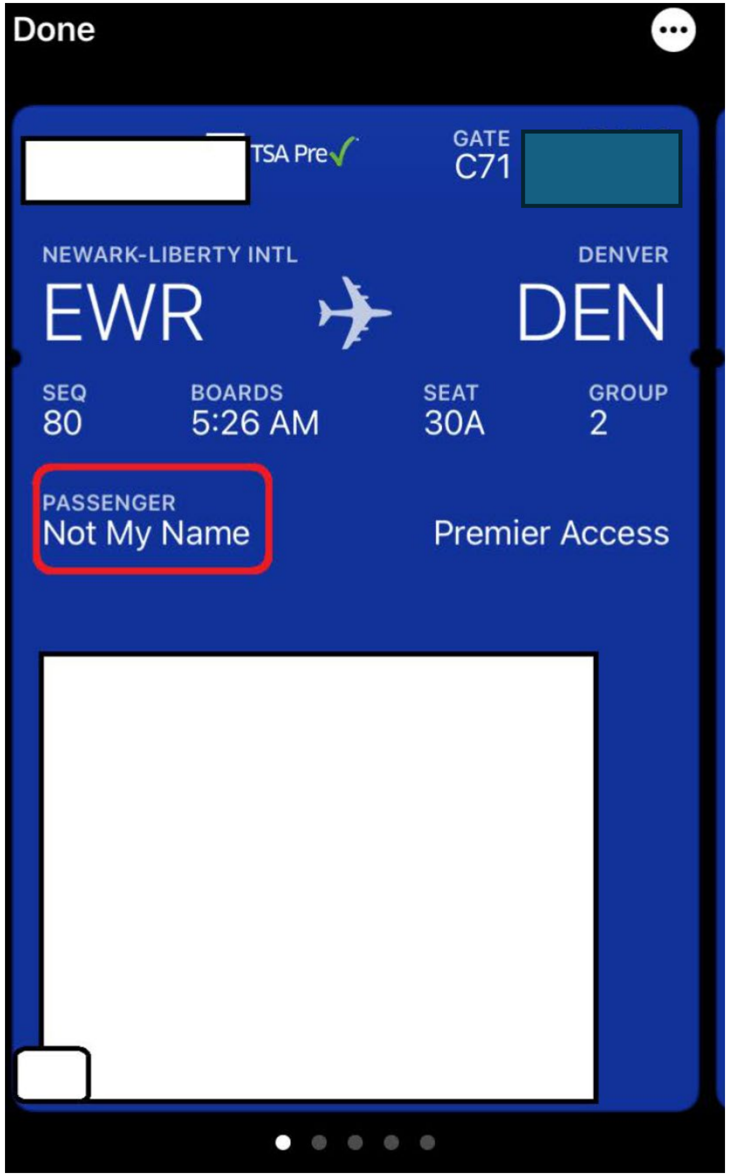
IHG ONE REWARDS

POINTS
120,000

PRIYANK NIGAM
248281972

STATUS
Diamond Elite

Huh?



Done

[redacted] TSA Pre✓

GATE
C71 [redacted]

NEWARK-LIBERTY INTL
EWR

DENVER
DEN

SEQ
80

BOARDS
5:26 AM

SEAT
30A

GROUP
2

PASSENGER
Not My Name

Premier Access

[redacted]

[redacted]

Case – Boarding Passes

The Bar Coded Boarding Pass (BCBP) standard covers the data and symbologies for paper or mobile devices to be used as boarding passes. However, it does not cover the distribution methods (how to send the barcodes to the devices) or other aspects of the implementation.

The following fields define a unique BCBP, without storing personal data:

- Date of flight (Julian date)
- Operating carrier code
- Flight number
- Check-in Sequence number
- From city / airport code

Encoding Algorithms for BCBP

2-D PDF417

Data Matrix ISO16022

Aztec ISO 24778

QR (Quick Response) Code

**https://www.qrcode.com/en/history/*

Case – Boarding Passes – QR Code

BAR CODED BOARDING PASS (BCBP) Structure

MANDATORY MANDATORY MANDATORY

```
M1NIGAM/PRIYANK    EXXXXXX   LHRFRALH   1651 220Y030A0080    15D>018 00

 W32XXBXX                2AXXXXXXXXX56270 UA LH LOYATYNO
```

OPTIONAL

```
^XX0MEQCIAmM48hDwD+p1r4nVY16DesRgBE37R/a0Xsk1x9puQ/eAiBXtXAQjuoJcyrPGtaEg
FMErrm3ynbuiA7SSRaFWLInrA==
```

Impact depends on the server aka the “reader”

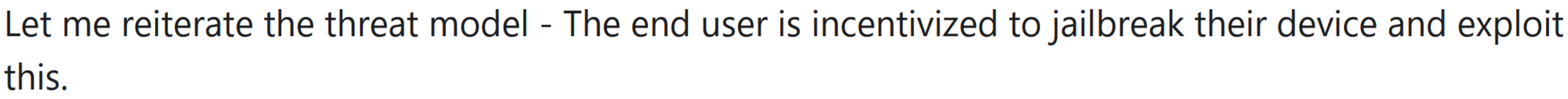
At the gate

At the Security Check

(Typical) Apple Response

“If you are able to demonstrate this issue on a non-jailbrok3n device, we'd be interested in investigating that scenario”

Me:



Let me reiterate the threat model - The end user is incentivized to jailbreak their device and exploit this.

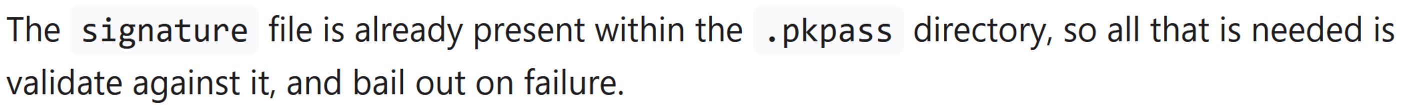
364
DAYS
LATER

Apple Product S3curity:

“We Apologize for our last messages and thanks for your reply.

Are you able to perform transactions or use any of your modified passes with live services? If so, which passes were successful and did the transaction use the modified valu3s?”

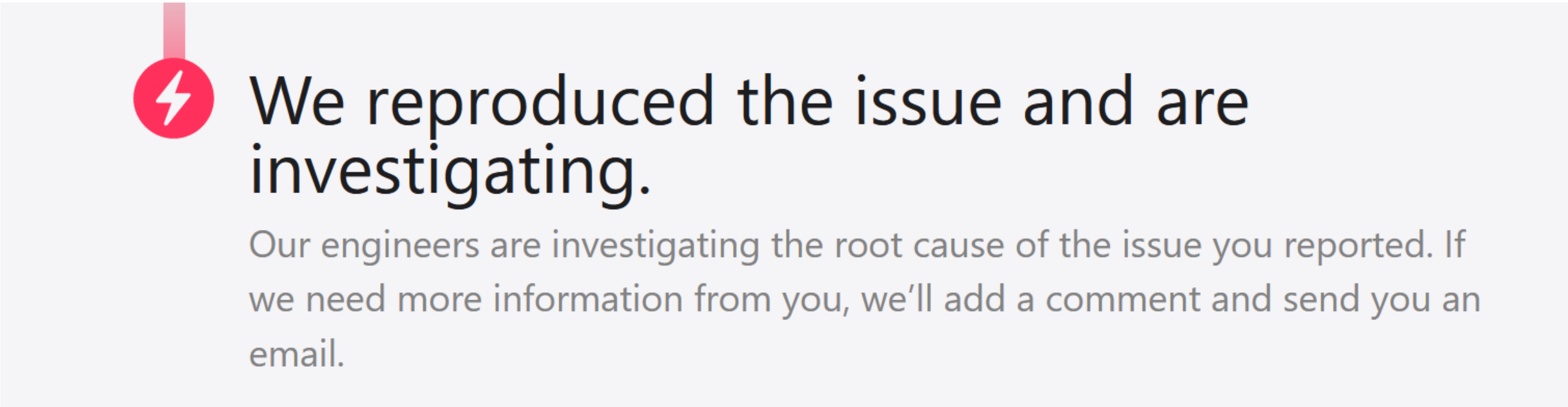
Me:



The `signature` file is already present within the `.pkpass` directory, so all that is needed is validate against it, and bail out on failure.

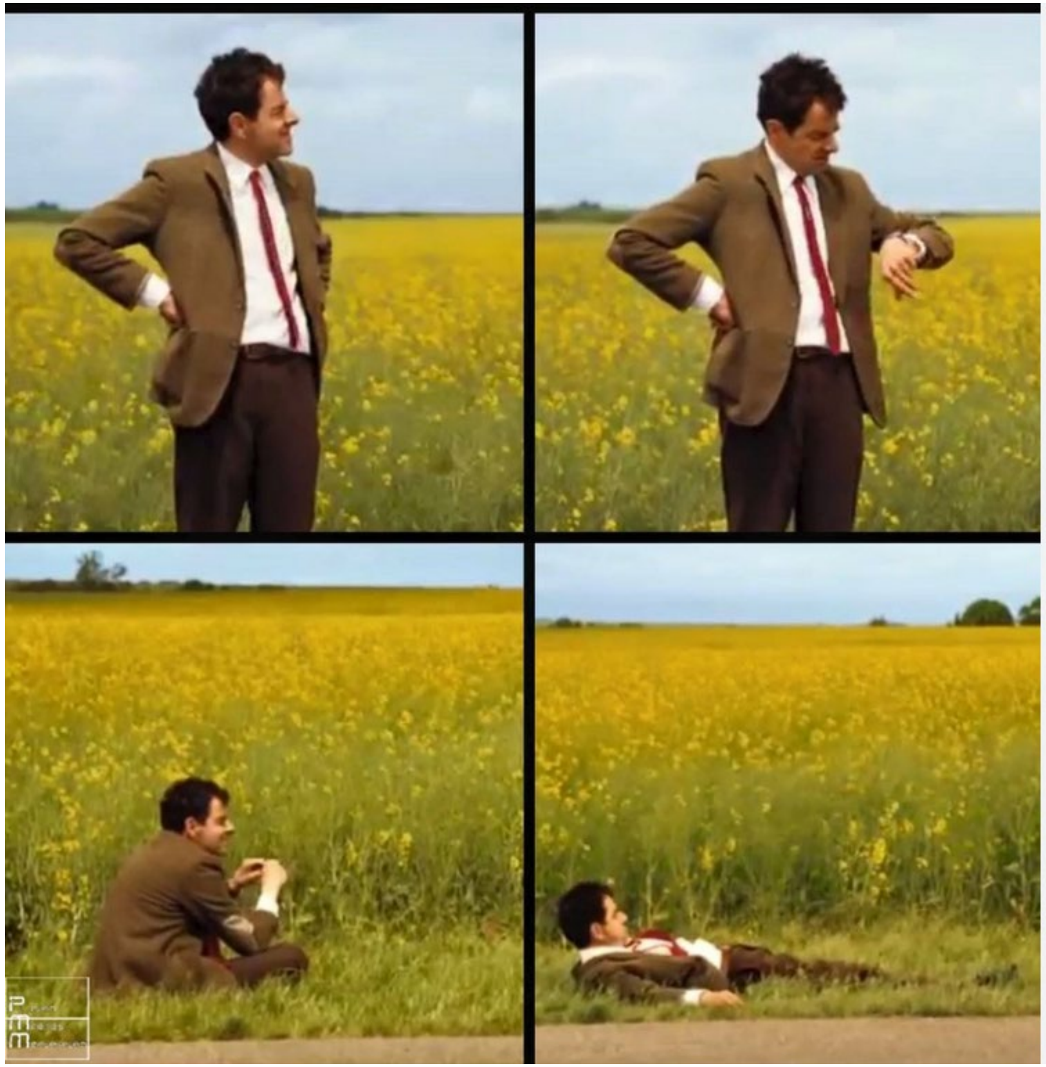
Apple can only verify the pass at the time it is loaded, since it does do the validation on pass installation (time-of-check-to-time-of-use); otherwise, the pass is essentially equivalent to a screenshot or a picture containing the same information, such as a boarding pass or a store card. Obviously, one is more credible than the other.

Ok..?



We reproduced the issue and are investigating.

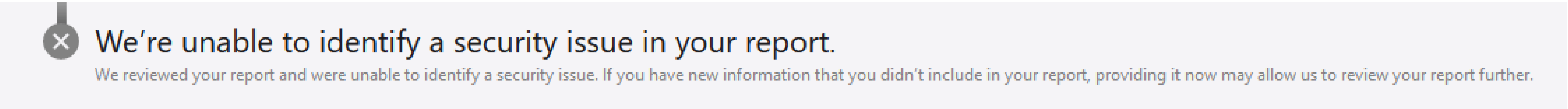
Our engineers are investigating the root cause of the issue you reported. If we need more information from you, we'll add a comment and send you an email.



Apple Product S3curity:

“We've investigated your report further and have forwarded it to the engineering team as a po1ential future enhancement.”

Later…



We’re unable to identify a security issue in your report.

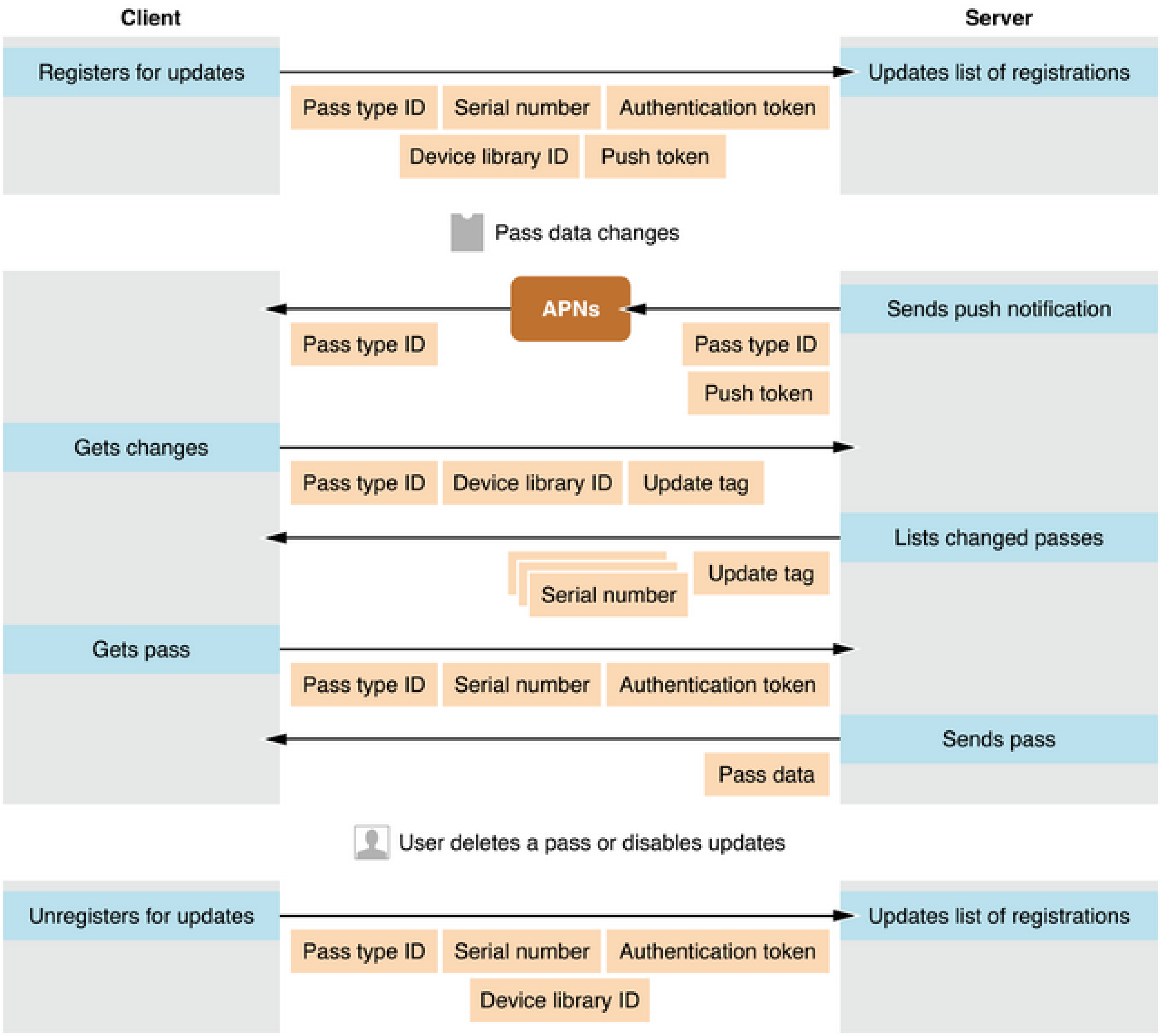
We reviewed your report and were unable to identify a security issue. If you have new information that you didn't include in your report, providing it now may allow us to review your report further.

Moving on..

- Apple being apple, has most likely pushed a fix, and will not credit the researcher.

- But WCGW even if this is fixed?

PKPass Updates



Authentication Token?

- Static for a vendor ☹

- The only secret is the serial#

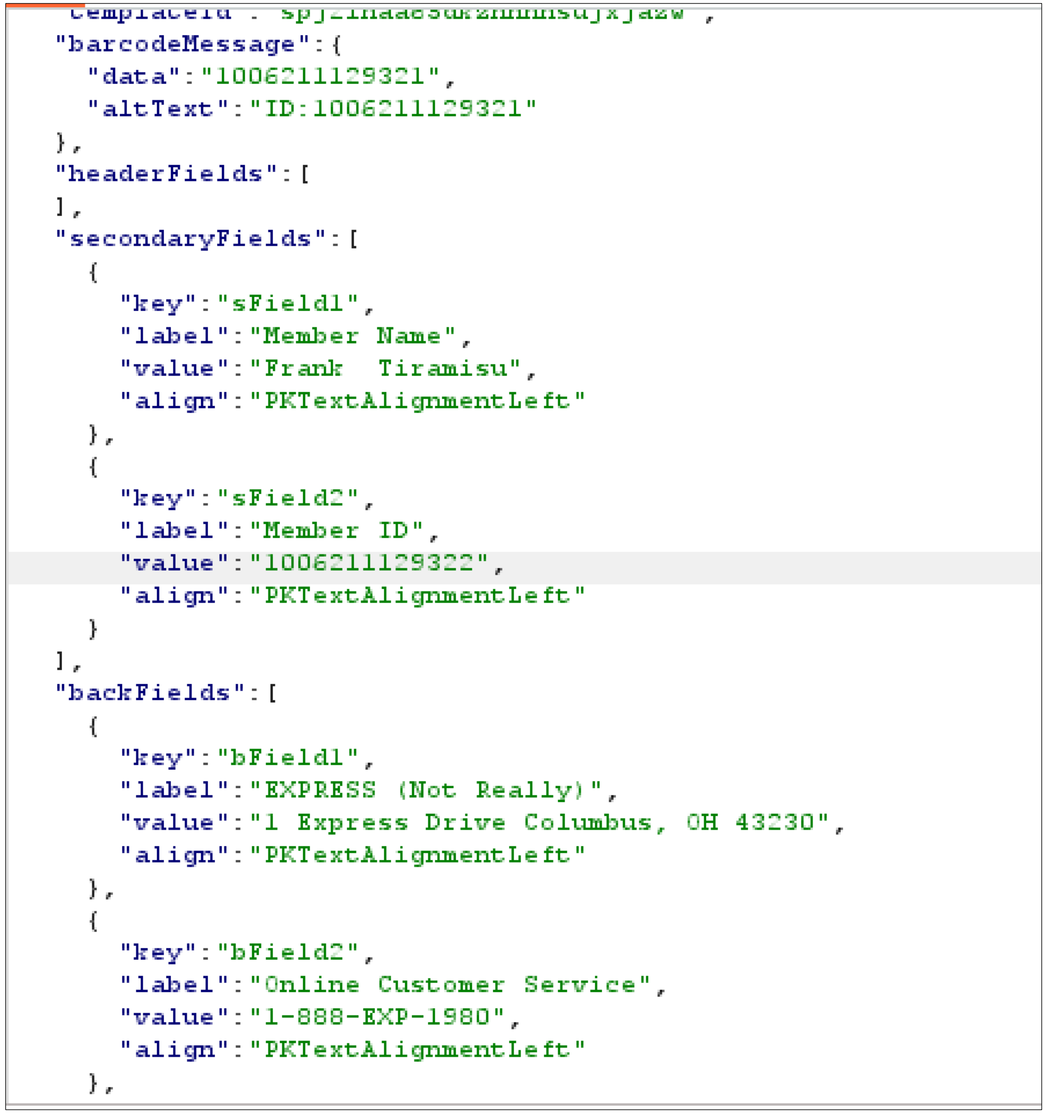
- UUIDs -> Secure
- Numeric identifier -> Not so much

- Attack the update API?

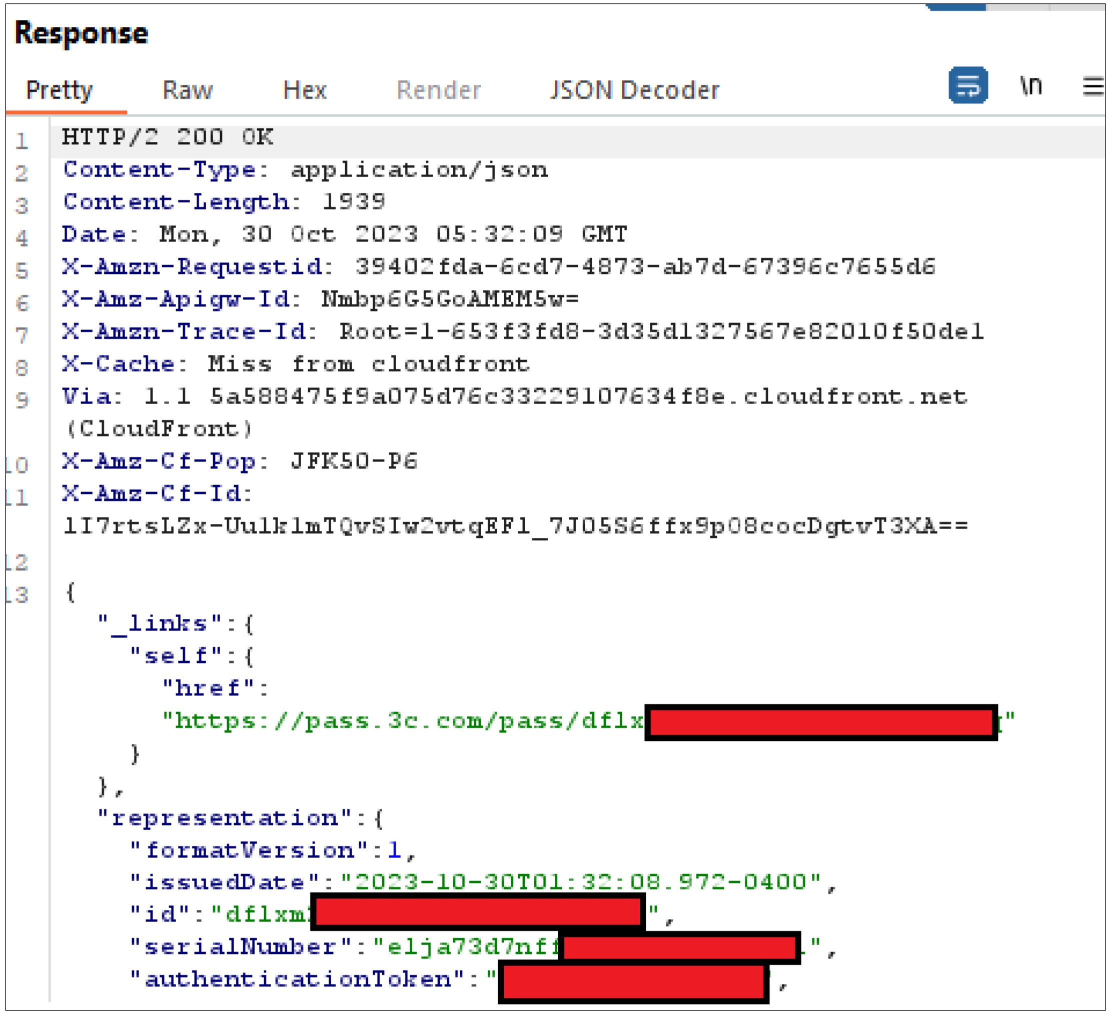
Forge the fields

- Can’t access other users’ PKPass but can forge your own?
- Mobile API to “generate” a PKPass? Obviously signed by the vendor

Whatever fields we want..

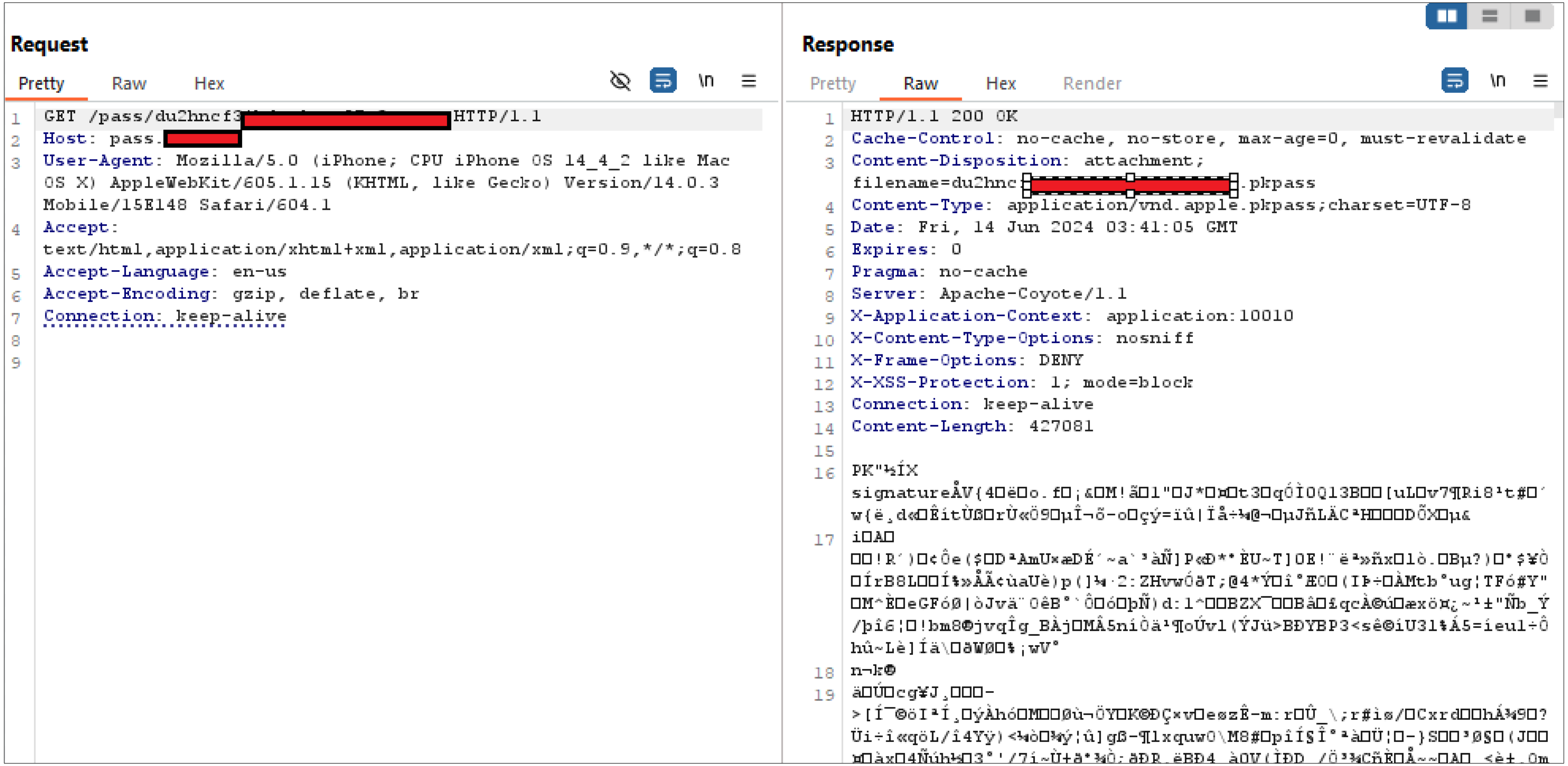


```
  "templateId":"spj2lnaa85dkznnnnsujxjazw",
  "barcodeMessage":{
    "data":"1006211129321",
    "altText":"ID:1006211129321"
  },
  "headerFields":[
  ],
  "secondaryFields":[
    {
      "key":"sField1",
      "label":"Member Name",
      "value":"Frank  Tiramisu",
      "align":"PKTextAlignmentLeft"
    },
    {
      "key":"sField2",
      "label":"Member ID",
      "value":"1006211129322",
      "align":"PKTextAlignmentLeft"
    }
  ],
  "backFields":[
    {
      "key":"bField1",
      "label":"EXPRESS (Not Really)",
      "value":"1 Express Drive Columbus, OH 43230",
      "align":"PKTextAlignmentLeft"
    },
    {
      "key":"bField2",
      "label":"Online Customer Service",
      "value":"1-888-EXP-1980",
      "align":"PKTextAlignmentLeft"
    },
```



```
HTTP/2 200 OK
Content-Type: application/json
Content-Length: 1939
Date: Mon, 30 Oct 2023 05:32:09 GMT
X-Amzn-Requestid: 39402fda-6cd7-4873-ab7d-67396c7655d6
X-Amz-Apigw-Id: Nmbp6G5GoAMEM5w=
X-Amzn-Trace-Id: Root=1-653f3fd8-3d35d1327567e82010f50de1
X-Cache: Miss from cloudfront
Via: 1.1 5a588475f9a075d76c33229107634f8e.cloudfront.net
(CloudFront)
X-Amz-Cf-Pop: JFK50-P6
X-Amz-Cf-Id:
1I7rtsLZx-UulklmTQvSIw2vtqEF1_7J05S6ffx9p08cocDgtvT3XA==

{
  "_links":{
    "self":{
      "href":
      "https://pass.3c.com/pass/dflx[redacted]"
    }
  },
  "representation":{
    "formatVersion":1,
    "issuedDate":"2023-10-30T01:32:08.972-0400",
    "id":"dflxm[redacted]",
    "serialNumber":"elja73d7nf[redacted]",
    "authenticationToken":"[redacted],
```

Download & Save



```
GET /pass/du2hncf3[redacted] HTTP/1.1
Host: pass.[redacted]
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_2 like Mac
OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.3
Mobile/15E148 Safari/604.1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us
Accept-Encoding: gzip, deflate, br
Connection: keep-alive


```

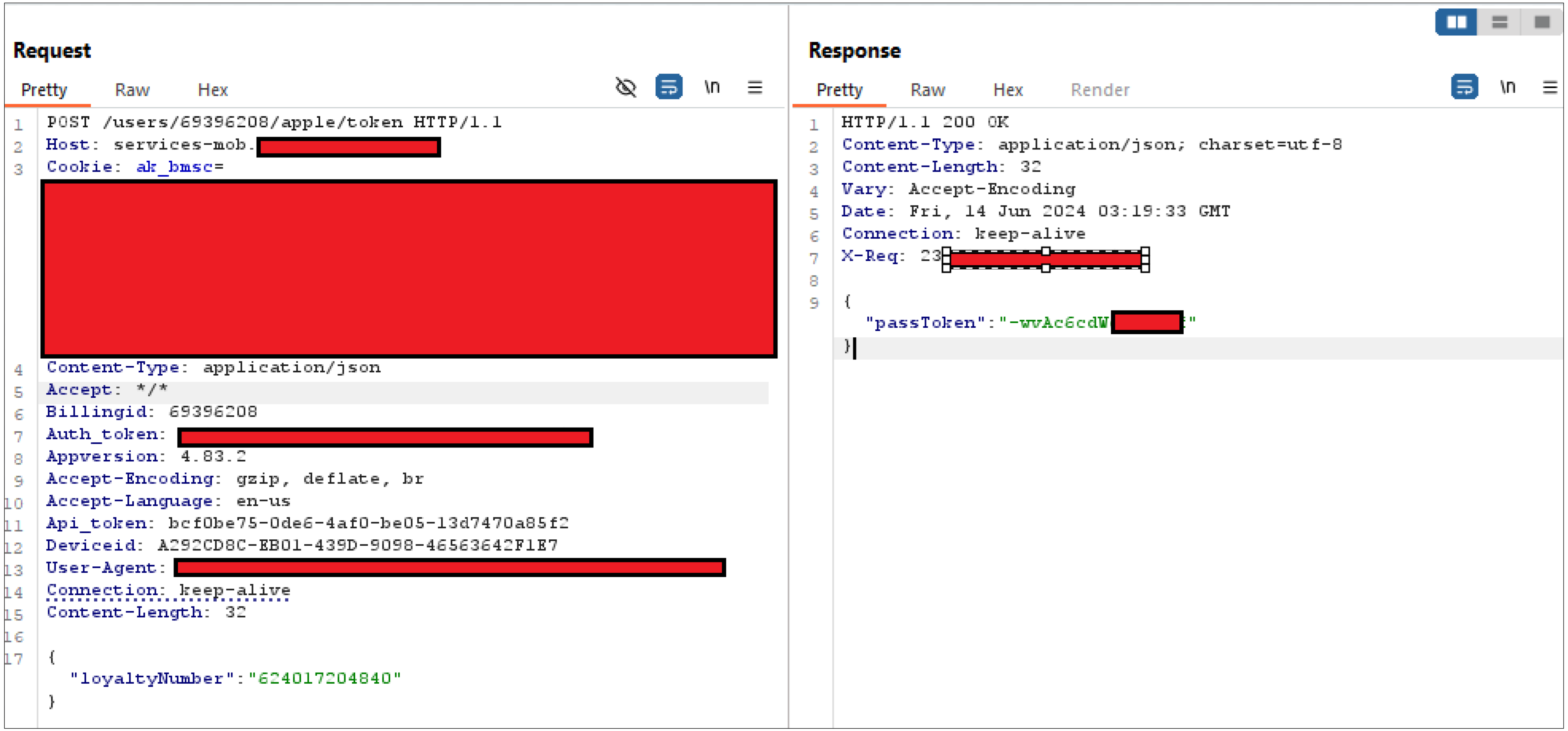
```
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Content-Disposition: attachment;
filename=du2hnc[redacted].pkpass
Content-Type: application/vnd.apple.pkpass;charset=UTF-8
Date: Fri, 14 Jun 2024 03:41:05 GMT
Expires: 0
Pragma: no-cache
Server: Apache-Coyote/1.1
X-Application-Context: application:10010
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
Connection: keep-alive
Content-Length: 427081

PK"¼ÍX
signatureÅV{4□ë□o.f□¡&□M!ã□1"□J*□¤□t3□qÓÌOQ13B□□[uL□v7¶Ri8¹t#□´
w{ë¸d«□ÊitÙß□rÙ«Ö9□µÎ¬õ-o□çý=iû|Ïå÷¼@¬□µJñLÄCªH□□□DÕX□µ&
i□A□
□□!R´)□¢Ôe($□DªAmU×æDÉ´~a`³àÑ]P«Ð**ÈU~T]OE!¨ëª»ñx□lò.□Bµ?)□*$¥Ò
□ÍrB8L□□Í$»ÅÃ¢ùaUè)p(]¼·2:ZHvwÓðT;@4*Ý□î°Æ0□(IÞ÷□ÀMtb°ug¦TFó#Y"
□M^È□eGFóØ|òJvä¨0êB°`Ô□ó□pÑ)d:1^□□BZX¯□□Bâ□£qcÀ©ú□æxö¤¿~¹±"Ñb_Ý
/þî6¦□!bm8®jvqÎg_BÀj□MÂ5níÒä¹¶oÚvl(ÝJü>BÐYBP3<sê©iU31$Á5=íeul÷Ô
hû~Lè]Íä\□ðWØ□$¡wV°
n¬k®
ä□Ú□cg¥J¸□□□-
>[Í¯®öIªÍ¸□ýÀhó□M□□Øù¬ÖY□K®ÐÇ×v□e¤zÊ-m:r□Û_\;r#i¤/□Cxrd□□hÁ¾9□?
Üi÷î«qöL/î4Yÿ)<¼ò□¾ý¦û]gß-¶lxquw0\M8#□pîÍ§Î°ªà□Ü¦□-}S□□³Ø§□(J□□
¤□àx□4Ñúh¼□3°'/7i~Ù+ã*¾Ò;ãÐR.ëBÐ4 àOV(ÌÐD /Ö³¾CñÈ□Å~~□A□ <è±.Om
```

Some airline..

```
POST /api/checkin HTTP/2.0
Host: app.airline.com
Content-type: application/json

…omitted for brevity…


{
“confirmation_no”: “XXXXXX”,
“priority_boarding”: true,

“message” : “M1/NAME/LASTNAME
^XX0MEQCIAmM48hDwD

“Seat” : “29A”,
“boardingGroup” “1”,
“status” : “Platinum”,
“isFastLane” : “true”,

}
```

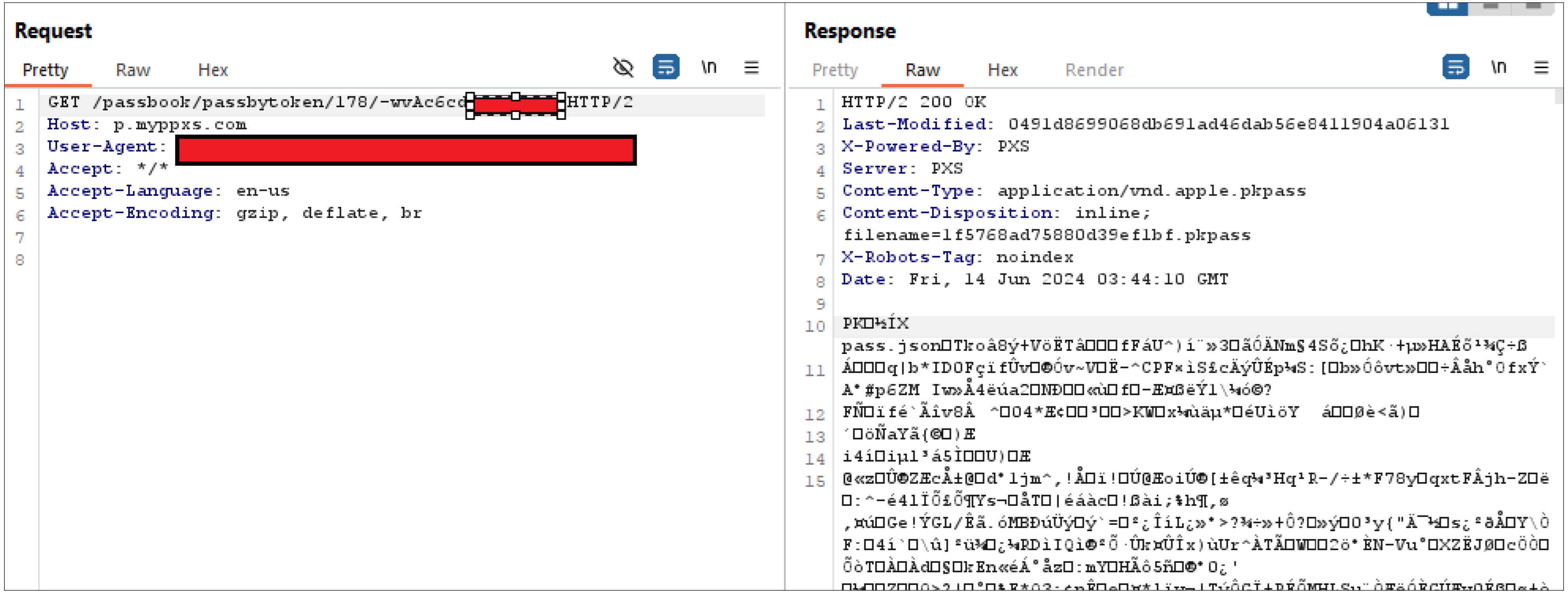
```
HTTP/2 200 OK
Content-Disposition: attachment;
filename=xnfc_pass.pkpass
Content-Type:
application/vnd.apple.pkpass;charset=UTF-8


PK<^WsignatureAVS
```

Can we “steal” passes?



```
POST /users/69396208/apple/token HTTP/1.1
Host: services-mob.[redacted]
Cookie: ak_bmsc=
[redacted]
Content-Type: application/json
Accept: */*
Billingid: 69396208
Auth_token: [redacted]
Appversion: 4.83.2
Accept-Encoding: gzip, deflate, br
Accept-Language: en-us
Api_token: bcf0be75-0de6-4af0-be05-13d7470a85f2
Deviceid: A292CD8C-EB01-439D-9098-46563642F1E7
User-Agent: [redacted]
Connection: keep-alive
Content-Length: 32

{
  "loyaltyNumber":"624017204840"
}
```

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Content-Length: 32
Vary: Accept-Encoding
Date: Fri, 14 Jun 2024 03:19:33 GMT
Connection: keep-alive
X-Req: 23[redacted]

{
  "passToken":"-wvAc6cdW[redacted]"
}
```



```
GET /passbook/passbytoken/178/-wvAc6cd[redacted]HTTP/2
Host: p.myppxs.com
User-Agent: [redacted]
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate, br
```

```
HTTP/2 200 OK
Last-Modified: 0491d8699068db691ad46dab56e8411904a06131
X-Powered-By: PXS
Server: PXS
Content-Type: application/vnd.apple.pkpass
Content-Disposition: inline;
filename=1f5768ad75880d39ef1bf.pkpass
X-Robots-Tag: noindex
Date: Fri, 14 Jun 2024 03:44:10 GMT

PK□¼ÍX
pass.json□Tkoâ8ý+VöËTâ□□□fFáU^)í¨»3□ãÓÂNm§4Sõ¿□hK ·+µ»HAÉõ¹¾Ç÷ß
Á□□□q|b*IDOFçïfÛv□®Óv~V□Ë-^CPF×ìS£cÄýÛÉp¼S:[□b»Óôvt»□□÷Âåh°0fxÝ`
A*#p6ZM Iw»Å4ëúa2□NÐ□□«ù□f□-Æ¤ßëŸ1\¼ó®?
FÑ□ïfé`Ãív8Â ^□04*Æ¢□□³□□>KW□x¼ùäµ*□éUìöY  á□□Øè<ã)□
´□öÑaYã(©□)Æ
i4í□iµl³á5Ì□□U)□Æ
@«z□Û®ZÆcÅ±@□d*1jm^,!Å□ï!□Ú@ÆoiÚ®[±êq¼³Hq¹R-/÷±*F78y□qxtFÂjh-Z□ë
□:^-é41ÏÕ£Õ¶Ys¬□åT□|éáàc□!ßài;$h¶,ø
,¤ú□Ge!ÝGL/Êã.óMBÐúÜý□ý`=□²¿ÎiL¿»*>?¾÷»+Ô?□»ý□0³y("Ä¯¼□s¿²ðÅ□Y\Ò
F:□4í`□\û]²ü¾□¿¼RDìIQì®²Õ·Ûk¤ÛÎx)ùUr^ÀTÃ□W□□2ö*ÈN-Vu°□XZËJØ□cÖÒ□
ÕòT□À□Àd□§□kEn«éÁ°åz□:mY□HÃô5ñ□®*0¿'
```

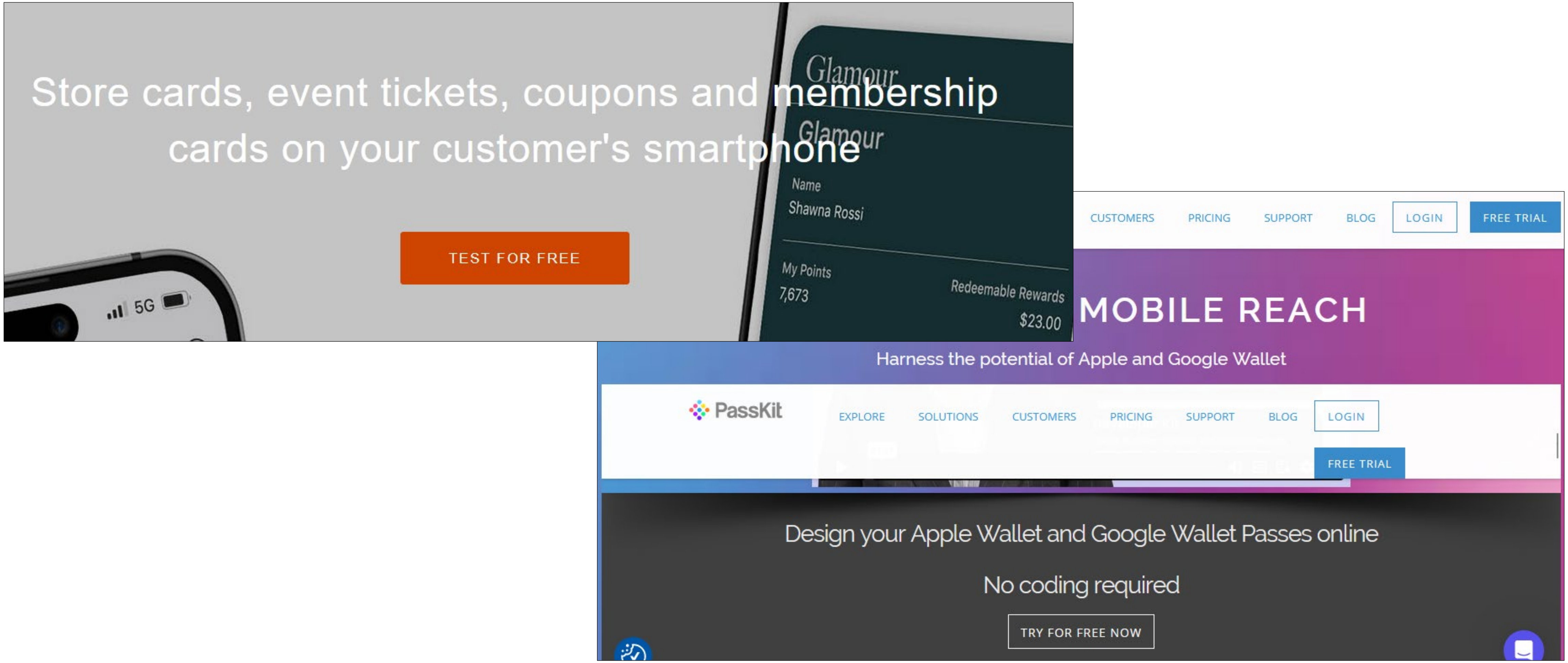
But Hold on..

All you need is a developer certificate to build your own!

To sign and compress the pass, use the official `signpass` tool to sign the pass package

```
$./signpass -p yolo.pass
```

Some Services will sign it for you (free/paid)



Store cards, event tickets, coupons and membership cards on your customer's smartphone

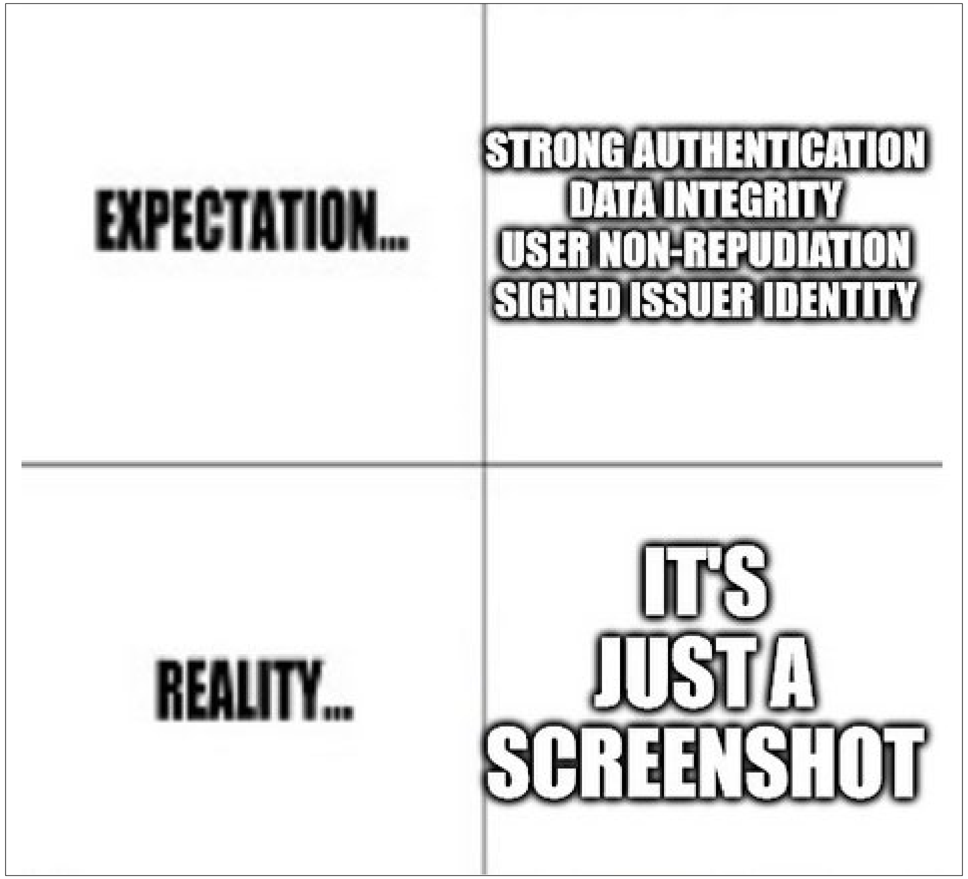
MOBILE REACH

Harness the potential of Apple and Google Wallet

Design your Apple Wallet and Google Wallet Passes online

No coding required

Conclusion



EXPECTATION...	STRONG AUTHENTICATION DATA INTEGRITY USER NON-REPUDIATION SIGNED ISSUER IDENTITY
REALITY...	IT'S JUST A SCREENSHOT

Wallet Apps Cheat Sheet

Issue	Solution
Business Use Case	**Seriously, what problem are you trying to solve?**
PKPass Generation	AppSec Best Practices 101 – Server-to-Server authentication
PKPass Delivery	Strong User Authentication/Authorization
PKPass Update	Strong identifiers/Dynamic authentication
PKPass Storage	Signed `message` field -> Don’t rely on Apple Limit end user PII, since any reader can read this info
PKPass Fields	Sensitive Information -> Accessible by end-user!
PKPass Validation	Online Verification, Challenge/Response protocol Verify the Signing Authority

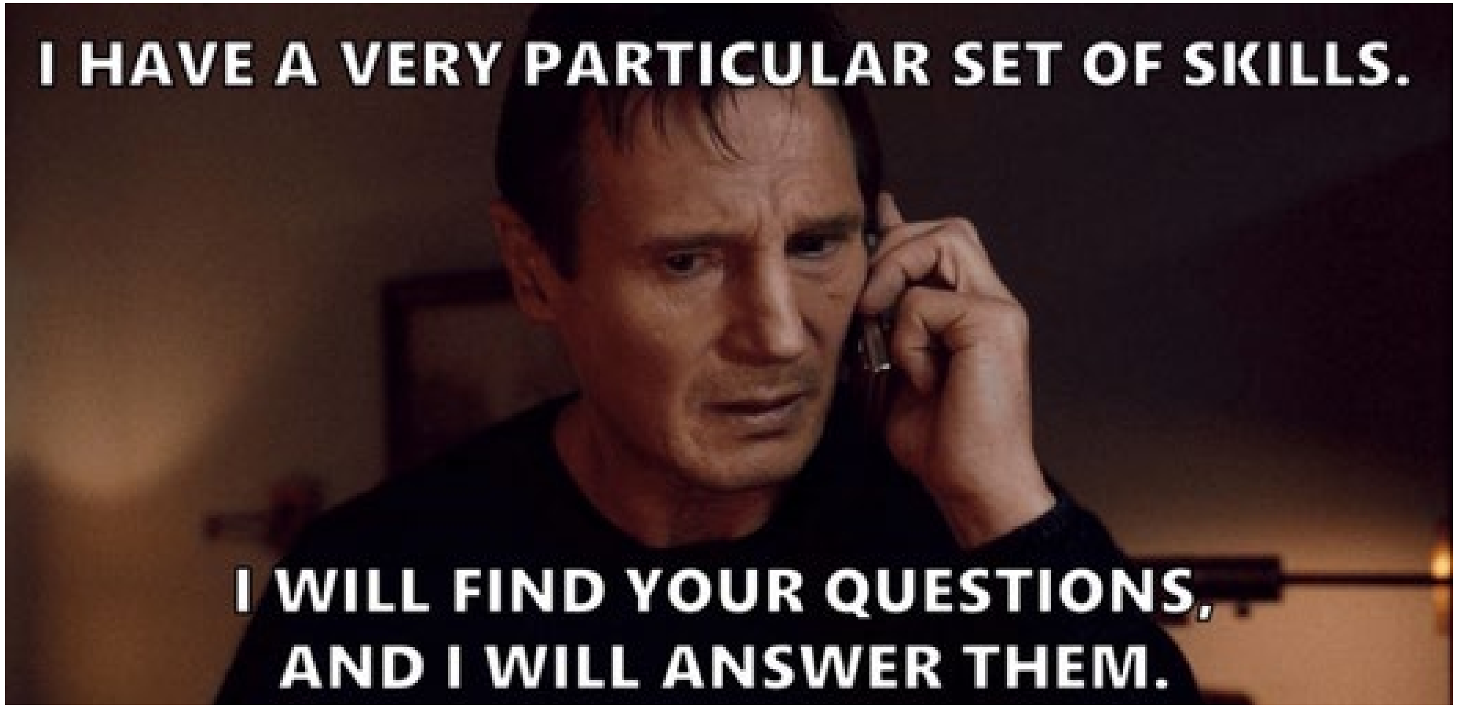
Questions/Feedback?

@Rev_Octo

Slides will be published later:
https://github.com/priyankn/Talks-Publications

Let’s connect!

https://linkedin.com/in/priyanknigam or scan below:


I HAVE A VERY PARTICULAR SET OF SKILLS.
I WILL FIND YOUR QUESTIONS, AND I WILL ANSWER THEM.