Cerner

code Learning Lab 2019

Best Practices for App Integration

Jenni Syed

Cerner

So you've built an app…

Before We Start

Things to not do

- Don’t cause a breach
  - Your app has access to PII and PHI
  - Your app has credentials

Protect your app and data

- Don’t post details on the web
- Don’t email requests/responses in the clear
- Authorization headers are secrets

Be aware of regulations

- Log files may contain PII, PHI
- Data shouldn’t transit in the clear
- Different localities, different rules (region, country, state, etc)

Where does the data go

- Some countries do not allow data to cross boundaries
- Some sites may require higher level protection

Being Educated

Know the spec?

- RTFM
  - No, not really

Know what is important

- Just in time
- Target to your functionality
- Overviews are a good place to start

Things to watch for

- Base spec rules
- Profiles and different implementations
  - Limits and special considerations

Being Flexible

Metadata

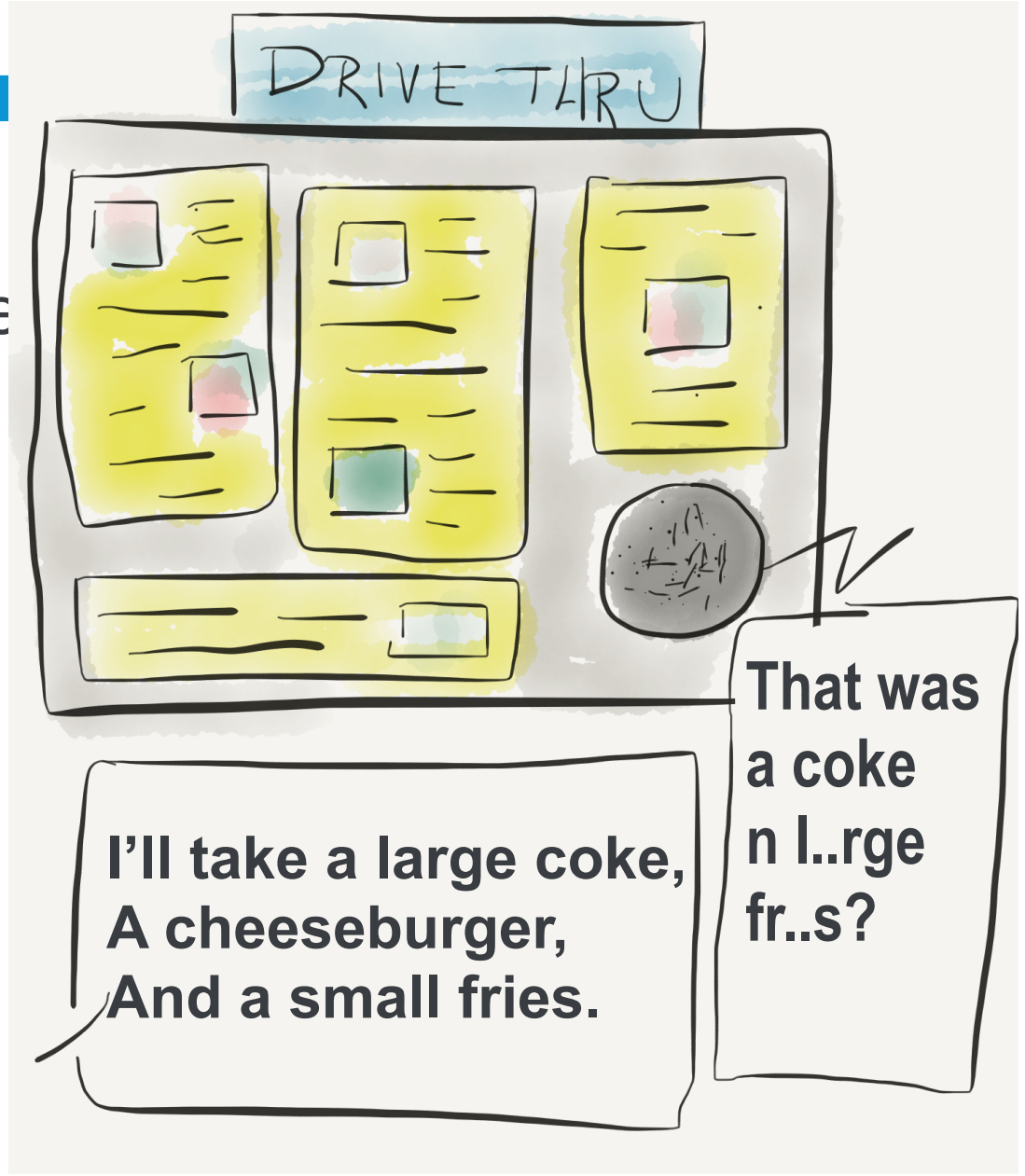
- Not just for OAuth
  - But yes, please for OAuth…
- Graceful Degradation
  - Resources, query parameters, actions

Graceful degradation

- Or progressive enhancement… you choose
- What is the minimum best experience that works for your app?
- What if a parameter isn’t available? What if a resource is not implemented?

OAuth

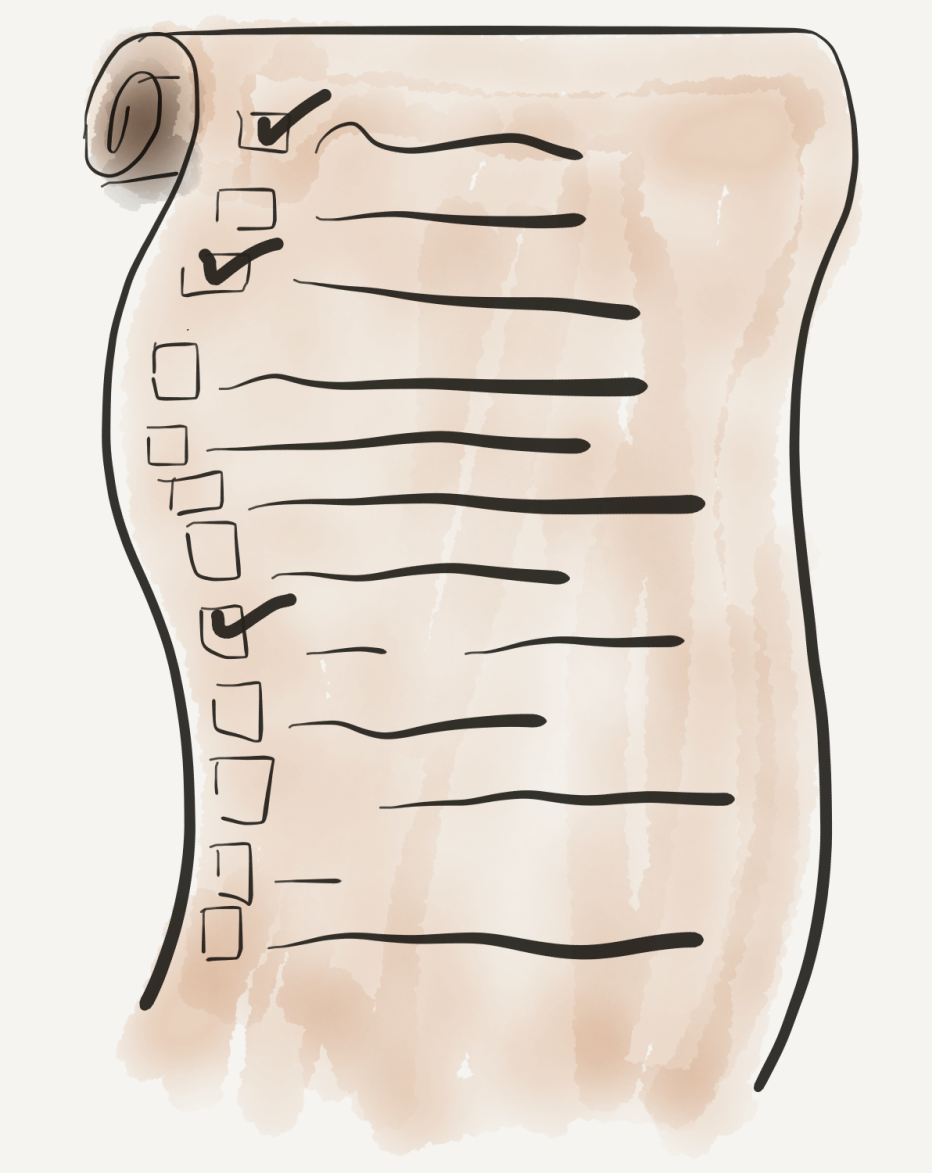
- Scopes returned as part of token
  - This is part of the base OAuth 2 spe
- 404 vs. readable error
  - Or graceful degradation?



Being Safe

There’s a checklist!

- Safety Checklist
  - https://www.hl7.org/fhir/r4/safety.html



Error handling

- What does your app do when something unexpected happens?
- For user facing: can they get to information to contact support?
- Does the app log errors (and details that can help)?
  - Be careful - don’t put sensitive info in insecure logs

Modifiers

- It’s complicated…
- But they’re important
  - These are fields your app needs to understand
  - (and part of the safety checklist)
- STATUS!!!

Writes

- Create:
  - Don’t blindly retry on error
  - The created id is returned in the Location header
  - Fields may not be recorded exactly as sent in

Writes: DocumentReference

- XHTML: strict
- Use the validators listed on our FHIR page
- Sanitization is done!
- See the doc for the attachment.data field
- https://fhir.cerner.com/millennium/dstu2/infrastructure/document-reference/#body-fields

Updates

- FHIR Rule: You must read before you write
  - An update includes *all* fields
  - Any field not populated should be deleted in the underlying system
- Patch:
  - App only sends in fields/changes it intends to make
- ETag:
  - The ETag header returned on a read is used on an update/ patch for optimistic locking via “If-Match” header
  - Don’t just re-read and apply

Being Secure

Don’t Get Hacked

- Whitelist
  - Why?
    - Protect your app
    - Protect the data
- State
  - Again, protect your app

Basic workflows

- Launch: Your app is sent a code and FHIR URL
  - The FHIR URL tells you where the auth server is
  - Do you trust the FHIR server you just called?
  - Is the auth server what you expected?
- Auth server redirects back to your app
  - Is the state what you expected (or is this coming from somewhere else?)
- Certificates

Principle of least privilege

- Use the right scopes
- Use the right authorization
  - B2B is not a workaround

Being Glocal

Glocalization

- Globalization, localization
- Especially for consumer applications
- Multilingual countries
- People travel?!?

What do you need?

- The spec allows for translations (https://www.hl7.org/fhir/r4/languages.html)
  - This does not affect dateTime, instant, number fields
  - Text, description, display, etc

What do you need?

- Defaults, narrative, and other translations (Oh my?)
  - “default” http://hl7.org/fhir/r4/resource-definitions.html#Resource.language
  - Narrative: http://hl7.org/fhir/r4/narrative.html#lang
  - Translations: http://hl7.org/fhir/r4/extension-translation.html
- Locale??

What else?

- The app displays
  - Do you need to worry about left/right?
  - Most devices or browsers have a default setting
- Displays you build from raw FHIR data
  - Numbers, date/times

Being Confident

Being Confident

- Multiple sandboxes
- Several reference servers available
- Which implementations will you support?

https://memegenerator.net

What to check?

- Confirm how the app handles:
  - Missing fields?
  - Different query params?
  - Different resources/missing resources?
  - Different authorization servers?
  - Errors returned from the servers?

Being Prepared

When specs attack!

- Things will go wrong.
- What do you expect the app to do when:
  - Connections fail?
  - Strange errors are returned?
  - Calls take longer than expected?

Things it shouldn’t do

- Infinite loading spinners
- Blank pages
- Everything looks great! (but the data is missing)
- Go down in flames
  - (unless your error page is FHIR themed)

Consider….

- How to alert the user
- Logging
  - Remember, be cautious with PII/PHI
  - Any special fields that can be logged out for troubleshooting?
- Troubleshooting
  - OperationOutcomes
  - http://hl7.org/fhir/r4/operationoutcome.html

Questions?