Mobile Developer Community Meetup

February 6, 2023

Agenda

- Land Acknowledgement
- Code of Conduct
- Developer Experience Team Update
- Presentation: Credential Management Best Practices
- Q & A

Land Acknowledgement

- I would like to acknowledge the land on which I am privileged to work, live and recreate on is the unceded territory of the Malahat people.

- I invite others who would like to, to share a territorial acknowledgment in chat or verbally.

Code Of Conduct

- Be kind and courteous.
  - Treat each other with empathy, respect, and dignity
- Respect differences of opinion
  - Remember that every design or implementation choice carries a trade-off and numerous costs
  - There is seldom a single right answer
- Remember that everyone was inexperienced at some point
  - We encourage people to learn and grow in a positive community environment

Developer Experience Team Updates

- Community Meetup Schedule
- Google Program
- Apple Developer Program
- Apple Enterprise Program

The Developer Experience Team

Karl Hardin
Senior Director, Digital Delivery

Jen Reiher
Senior Product Manager

Shea Phillips
Architect

Shiho Itagaki
SaaS Manager

Edson Naves
Scrum Master

Martha Edwards
Lead Service Designer

Monica Granbois
Mobile App Devops Specialist

Galen Gray
Technical Community Manager

Community Meetup Schedule

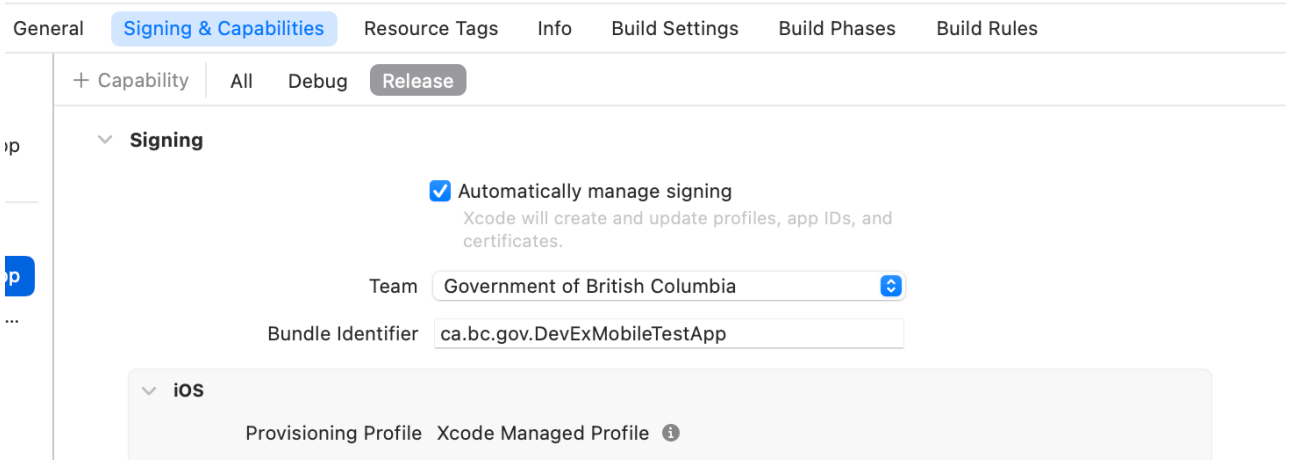
- Quarterly meetups with this year's dates as:
  - Feb 6th @1pm (Q4)
  - May 8 @1pm (Q1)
  - Sept 11 @1pm (Q2)
  - Dec 4 @1pm (Q3)

Google Program

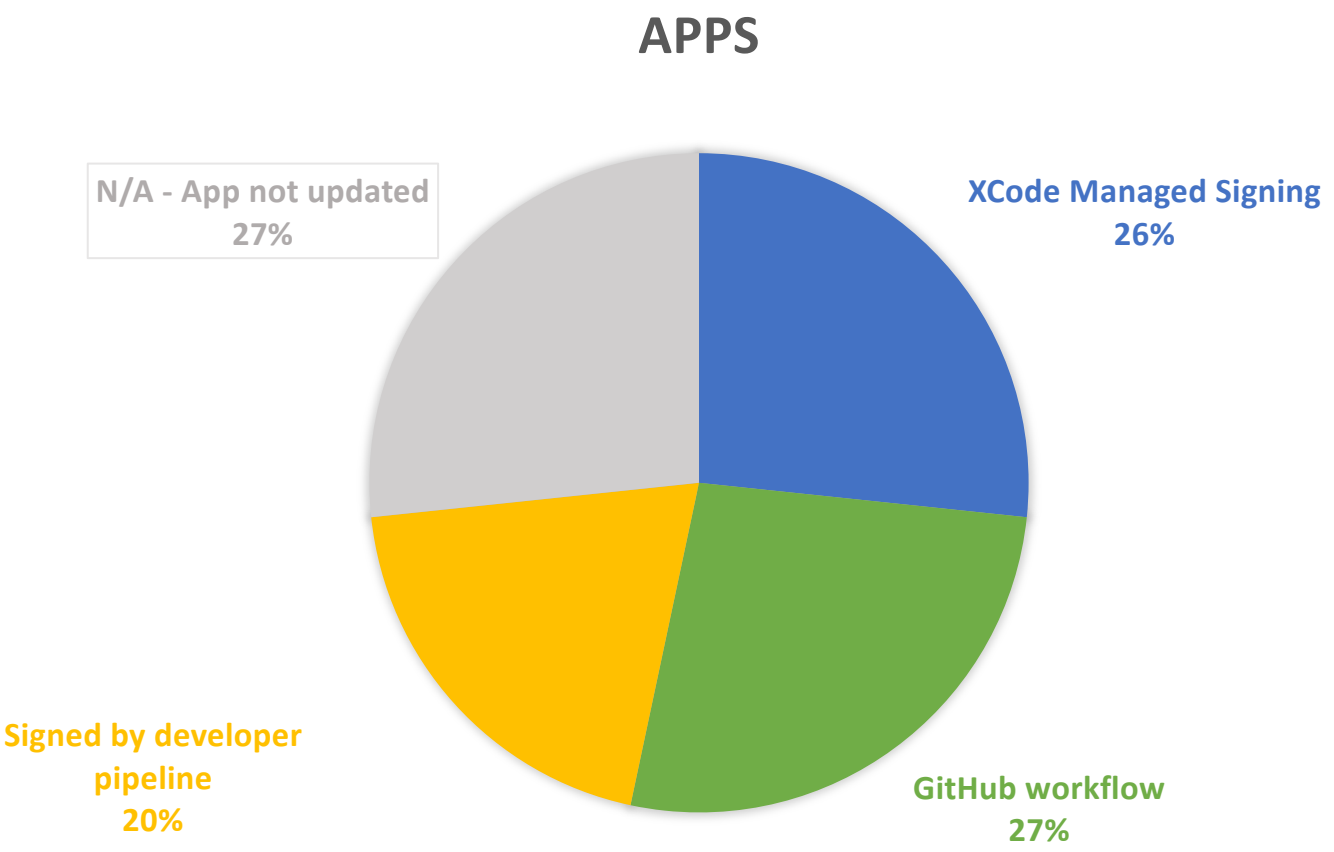
- Google Play Console is now requiring account verification
- Developer Experience Team is handling this verification
- We have set our verification date (Sept 26, 2024)
- No action required by app teams

Apple Developer Program

- September 2023 - turned on “XCode automatic manage signing”
  - 4 apps moved to this method
  - 15 apps are listed on the Apple App Store



App Signing Process



App Signing

- We will work with teams to move to either the xcode managed or a GitHub workflow as apps move back into development

Apple Enterprise Program

- The account has been renewed for another year
  - We go through a yearly application process to renew our subscription in the Enterprise program
- Updated documentation in the mobile developer guide to include more details on enterprise and custom app distribution methods
- Worked with teams to revoke and reissue compromised signing certificate

Certificate Revocation – The Issue

- The Enterprise certificate and associated provisioning profile was checked into the public bcgov GitHub organization

Certificate Revocation – The Risk

- Apps signed by the enterprise certificate can run on any iOS device.
  - This is different than the Apple Developer Certificate. Signing with that certificate allows uploads to the App Store Connect account. Apple resigns all apps with its certificate when released to the app store
- This means a bad actor could release an app that would run on a user's device that looks like it was created by us
- We could not immediately revoke the certificate because it would cause all enterprise apps to stop working

Certificate Revocation Timeline

- Monday January 15
  - Learned of certificate and provisioning profile checked into public GitHub repo
  - Notified app team and asked them to remove the files
  - Notified Nick Corcoran, Security Architect with OCIO
  - Nick escalated to CITZ Information Privacy and Security
- Wednesday January 17
  - CITZ Information Privacy and Security recommends revoking the certificate
  - Email communication drafted
- Thursday January 18
  - app team completes removing certificates from all branches and histories
  - Email sent to all Enterprise app teams

Certificate Revocation Timeline

- Thursday January 18 - Monday January 22
  - Meeting or email discussion with teams about the issue
- Thursday January 18 - Thursday January 25
  - Teams update apps to use new provisioning profile/certificate
  - Apps given to Mobile Device Management team to distribute via MDM inTunes
- Friday January 26
  - Certificate is revoked

Certificate Revocation Timeline

- Thank you everyone for your quick response!

Certificate Revocation Timeline – Next Steps

- Developer Experience Team will work with teams to either:
  - Move to Apple Custom App on the Apple Developer account
  - Move to a pipeline where we can place the certificate in a secret store
  - We do not want to send the certificate to developers as was done in the past

Presentation from Nick Corcoran

Credentials Management
Best Practices

Credentials Management Best Practices

Nick Corcoran
Security Architect
DevOps and Cloud Services

Feb 2024

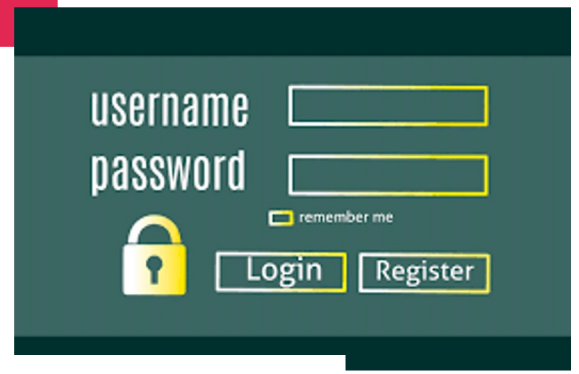
We'll talk about …

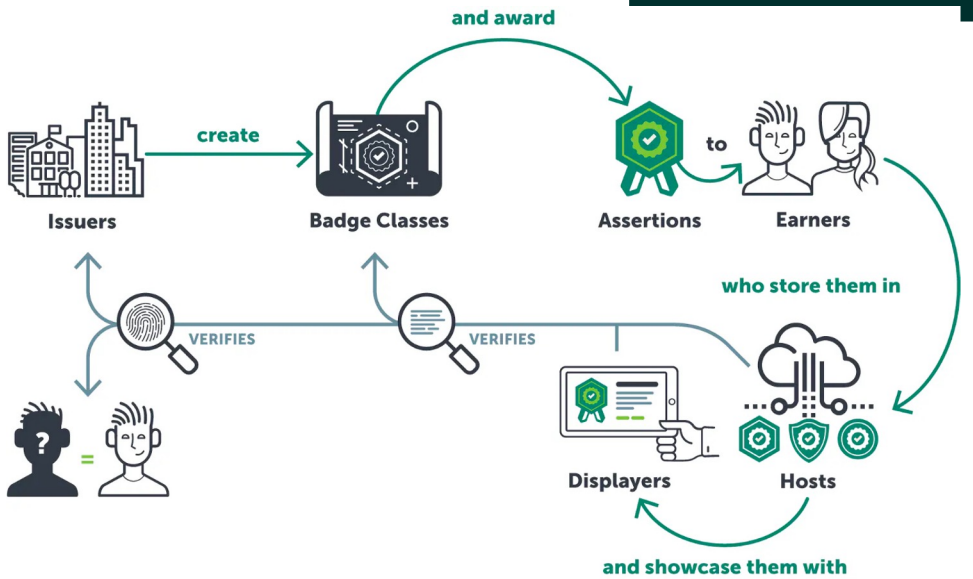
- What are credentials?
- Where can I store/access secrets during development?
- Why do I need to sign my app with a certificate?
- Who do I call if I notice something not right or I made a mistake?
- What happens when we don't properly control secrets?
- Questions

What are credentials?

Elements that permit access to a resource:

- usernames,
- passwords,
- certificates,
- keys, and
- biometric statistics.





Where to put my *******?

GitHub Secrets (limited to 48kb)

Secrets Manager (local, online)

Private storage (S3, private repo, OCIO key mgmt service - not yet available)

Don’t put secrets in code

Don’t put secrets files in public repos

Why should I care?

Certificates

To help ensure that all apps **come from a known and approved source** and **haven't been tampered with**, **iOS** and iPadOS require that all executable code be signed using an **Apple-issued** certificate.

Android requires that all apps be digitally signed with a certificate before they can be installed. Android uses this certificate to **identify the author of an app**, and the certificate does not need to be signed by a certificate authority. Android apps often use **self-signed** certificates.

Help?

7-7000 Option 3
Tell your **supervisor**
Tell your **MISO**
Tell **Monica** or **Nick**

It’s no longer a secret….

Report

- What was it?
- Where was it?
- Who had access?
- Impact?

Containment/Recovery

Remediation

Prevention


Thank
You

Questions

Next Meetup Teaser

The BC Wallet App team will present on their app development/deployment flow