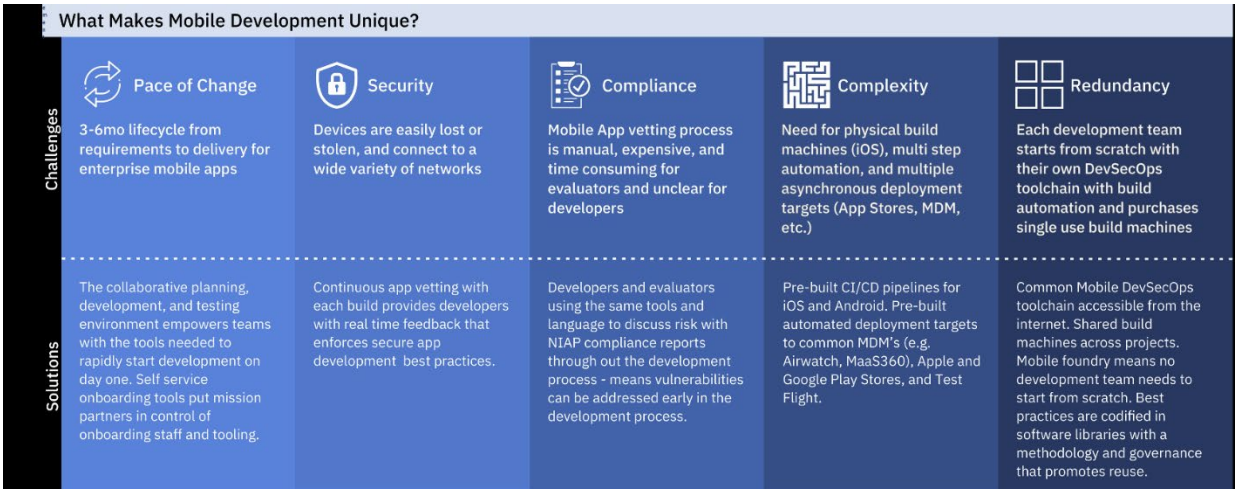
1 The Capability Gap - Addressing the Executive Order (EO) Areas 2 & 4: Software Development Lifecycle Standards (SDLC) & Requirements for Testing - EO Section 4(e)(i, ii, iv, v, ix, and x) and 4(r)

Ensuring adherence to SDLC Standards is a challenge for all government agencies in the mobile space. One major component of this challenge is the disparate set of tooling adopted by different organizations, and even different development teams within a single organization. It is time consuming and expensive to validate the complete system when comprised of a large set of interchangeable components. We propose to simplify the management and validation of the SDLC tooling by providing an exemplary, fully scoped, environment which can combine the disparate tooling to a single view.

Currently the most widely adopted standard for mobile application development in US Government is the National Information Assurance Partnership (NIAP) Protection Profile (PP) for Application Software. This remains the best choice for application software standards but has significant challenges before it can be adopted across the government. The time and cost of certification does not scale with the rapid pace of development for mobile applications, an automated and integrated testing solution is proposed to address this challenge.

2 Closing the Gap - Current Challenges In Detail

Mobile application development is unique in comparison with back-end, web, or desktop development - and It is uniquely challenging. The figure below shows the core challenges in detail along with the solutions which outline best practices and guidance throughout the mobile application development lifecycle.



2.1 Key Components

2.1.1 DevSecOps Toolchains

IBM Services Essentials is a comprehensive DevSecOps integration platform that brings together various tools – both open-source and licensed – into a common platform with a single unified experience to act as a “one-stop shop” for Agile mobile application development.

IBM’s approach to DevSecOps is not one of reimplementation or a proprietary stack, but one of integration of the best tools already available on the market – the same tools that are being used by developers all around the world today – and bring them together into a seamless whole and a Single Pane of Glass experience.

At the core of IBM Services Essentials is Boomerang Flow, a graphical orchestration tool that allows developers to define and customize their CI/CD toolchain through drag-and-drop mechanics. Boomerang Flow allows development teams to not only indicate how their tools should interact, but also set quality gates on build promotion. For example, a development team may set a gate that would indicate that a build cannot be deployed to the Quality Assurance (QA) team unless their integrated unit testing tool reports 100% success and the team’s integrated static code analysis tool (e.g. SonarQube) reports no major code flaws.

As part of its Single Pane of Glass philosophy, IBM Services Essentials also aggregates reports from its integrated tools as well as its CI/CD orchestration into a single reports pane, giving product owners and stakeholders visibility into overall code quality and development performance from a single dashboard, rather than having to manually tie together reports from all the different tools individually.

2.1.2 Mobile Accelerators

IBM Services Essentials' Accelerators (also called the Code Foundry) allows development teams to harvest, curate, and share their best hardened and proven assets through the platform, allowing teams to develop applications faster, rather than spending time implementing the same code over and over again.

2.1.3 Security & Compliance Testing

Kryptowire has developed mobile application testing engines in collaboration with the government's advanced research arms including DARPA, DHS, and NIST for over 10 years. The proprietary analysis systems that were developed in this partnership provide the only automated, closed-loop, Android & iOS testing solution which supports all major testing types.

Integration of the Kryptowire Android & iOS analysis systems into IBM Services Essentials enables stakeholders to meet and exceed the testing requirements outlined in the EO. Kryptowire's technology has undergone a capability review by the creators of the NIAP standard in collaboration with DHS and is the only solution proven to meet the technological requirements needed to support NIAP compliance testing. The testing is automated as a step in the build process through IBM Services Essentials and executes every time a developer makes a change to the application codebase. By automating this process, vulnerabilities are identified as early as possible in the development lifecycle and developers code for NIAP compliance from the very beginning.

3 Previous Implementation – DISA Mobile Enablement Prototype (2020-2021)

In response to the Statement of Need from the MEP OTA (8/2019), IBM partnered with Kryptowire to provide DISA with the same cloud-based DevSecOps toolchain that IBM uses internally to deliver over 300 mobile apps to our customers both commercial and government. NIAP compliance testing currently is conducted manually and traditionally taking between 90 days and 6 months. This means a new mobile capability takes between 8 to 18 months to be deployed. The Mobility Enablement Prototype project showcased that NIAP compliance testing takes minutes instead of months and happens with every build during the development cycle. Additionally, using the IBM Services Essentials platform, the project team delivered 3 NIAP complaint apps on both iOS and Android in less than 5 months. The process, people, tools, and governance working in tandem foster an environment where critical outcomes, such as speed of execution and continued compliance, can be achieved by DISA and their mission partners.

The mobile application development process from onboarding to development, compliance/authorization, and onto Production has a positive impact on several groups of stakeholders including Information Assurance, mobile app developers, and the mission partners utilizing the systems / applications. The figure below illustrates the journey of each of the core stakeholders, the capabilities, tooling, high level outcomes, and benefits to each stakeholder group.