IT@Intel White Paper

Intel IT
Mobile Application Development
July 2013

Implementing a Cross-Platform Enterprise Mobile Application Framework

The framework enabled us to develop and deploy a new mobile application in just a few weeks by reusing client runtime libraries, back-end functionality, approvals, and firewall and gateway configurations.

Arijit Bandyopadhyay
Enterprise Architect, Intel IT

Omer Ben-Shalom
Senior Principal Engineer, Intel IT

Krishnan Saikrishnan
IT Manager, Intel IT

Samion Kuptiev
Software Development – Team Lead, Intel IT

Executive Overview

Intel IT is extending an enterprise mobile application framework to support cross-platform mobile application development. The framework lays the foundation for rapidly taking advantage of emerging technologies, such as context-aware computing, and interaction methods, such as perceptual computing.

The framework consists of a standardized development environment, a secure runtime environment, an API aggregation gateway, and mobile management. It provides application developers with reusable building blocks for accessing local device capabilities and back-end services, enabling them to focus on user experience (UX) and business logic. For example, authentication and security are handled by the runtime environment within the client-side application—developers do not have to rewrite these pieces of code for every application.

Our extended framework offers enterprise-wide benefits:

- End users benefit from device flexibility and UX consistency. As a user switches between applications on the same device or between devices to access the same application, the framework allows the UX to remain consistent and yet take advantage of the specific device's capabilities.
- Application developers benefit from reusable user interface controls, fast application development and deployment, and workflow capabilities that insulate them from infrastructure provisioning and interfaces to back-end services. The framework also allows changes in infrastructure, such as the authentication method, without changes in code.
- Business groups benefit from fast application development and templates that are based on Intel business processes and aligned with corporate UX guidelines.
- Administrators benefit from a unified security model across all device types, scalability for fast provisioning and revocation, flexibility to add new device types, and dynamic policy enforcement.

The framework enabled us to develop and deploy a new mobile application in just a few weeks by reusing client runtime libraries, back-end functionality, approvals, and firewall and gateway configurations.

Contents

IT@INTEL

The IT@Intel program connects IT professionals around the world with their peers inside our organization – sharing lessons learned, methods and strategies. Our goal is simple: Share Intel IT best practices that create business value and make IT a competitive advantage. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

BUSINESS CHALLENGE

We are building an infrastructure that can take advantage of mobile-device capabilities and Intel® technologies such as hardware acceleration and identity protection. This infrastructure will also be able to support context as a service,[1] trust as a service, and other service interfaces. Developing this infrastructure will enable us to take advantage of the adaptive applications and digital assistants of the near future that will combine consumer and enterprise services in a just-in-time manner, creating new value for Intel employees.

Employees bring a wide range of connected devices, such as smartphones, tablets, laptops, and business Ultrabook™ devices, into the enterprise and expect to be able to access enterprise applications and services regardless of their choice of device and location. To meet this expectation, Intel IT must develop a secure, affordable, and scalable framework to build, deploy, and sustain mobile applications on various form factors and OSs, and on corporate and personally owned devices. We also want to enable employees to use new perceptual UIs such as touch, voice, gesture, and eye tracking, and—in the future—emotion detection and voice-intonation detection. Our goal is to enable seamless access to services and data from multiple devices while maintaining enterprise security.

The Evolution of Mobile Application Development

As the number of mobile applications continues to grow, the historical model of developing an application for a specific device cannot adequately scale to meet demand.

[1] See "Creating Business Value through Context-Aware Computing," June 2013.

The complexity of mobile applications has increased, and a per-device approach is no longer viable because it can lead to the following problems:

- Duplicate development efforts
- Use of proprietary programming languages
- Increased time-to-market
- Inconsistent experiences for developers, testers, and end users.

In response to these problems, the industry attempted to standardize on the use of web-based code, especially HTML5, with web interfaces running in portals. However, that approach encouraged a lowest-common-denominator user experience (UX) and application functionality—and end users were dissatisfied. Consequently, the industry began developing mobile enterprise application platforms (MEAPs). These products are a comprehensive suite of tools and services that enable development of mobile applications.

The next step in mobile application development—the mobile application development platform (MADP)—is software designed to support rapid development and deployment of mobile applications. We believe that an MADP-based approach to mobile application development can bring significant advantages to the enterprise, including the following:

- Increase the speed of developing mobile applications for all platforms
- Encourage a consistent UX
- Provide a robust security framework
- Enable better data connectivity
- Provide management and reporting capabilities

Mobile Application Development Challenges

Cross-platform application development is particularly challenging in a complex computing environment such as Intel's, which includes several OSs, form factors, and models of device ownership. Each device and OS uses different methods to implement similar capabilities, which are often optimized for a particular platform. Accordingly, developers have historically created separate mobile applications for each platform, resulting in an extended time-to-market, fragmented development skills, and substantial challenges in maintenance and support.

In addition to creating support and manageability issues, cross-platform development requirements have challenged us to achieve the following:

- Provide a consistent development environment that can be used to develop and deploy applications on all platforms in use at Intel
- Provide a specialized runtime environment that can interface with native device capabilities and make use of the richer UX they make possible
- Meet Intel's information security requirements across a range of IT-managed devices and personally owned devices, while supporting developer and customer needs
- Enable applications to access enterprise back-end resources, such as web services and code libraries, through a standard set of methods
- Engage developers in a cross-platform effort to help solutions become more robust and comprehensive

We kept these challenges in mind as we considered the application delivery mechanisms shown in Figure 1. We wanted an approach to mobile application development that supported both ease of development and a rich UX. Whenever possible, we prefer to deploy applications using either a hybrid combination of native HTML5 code and web browser or the web browser. Our goal is to use these deployment mechanisms for about 80 percent of mobile applications.[2]

Using a hybrid approach based on HTML5, we retain the ease of development common to web-based applications without sacrificing the rich UX common to native application development. We evaluated several MADPs and chose one as the basis for an enterprise mobile application framework that meets Intel's enterprise requirements.

[2] For more information on our choice of deployment mechanisms and their advantages and disadvantages, refer to the IT@Intel white paper, "Building a Mobile Application Development Framework."

INTEL'S ENTERPRISE MOBILE APPLICATION FRAMEWORK

Our cross-platform enterprise mobile application framework is built on an MADP using standardized technology capabilities such as HTML5 and CSS3 rendering. We supplemented the MADP with additional capabilities such as authentication, API connections to device-specific features, and encrypted communications.

This extended framework enables us to provide a fast-track mobile application development and deployment capability that can keep pace with the rapid introduction of form factors, interaction methods, and OSs. This solution also provides mitigating capabilities and the ability to grant or revoke appropriate access levels, which address the common challenges that enterprise IT departments face with respect to data security, privacy, and device manageability.

One added benefit of using HTML5 is that business groups no longer need to hire expert developers skilled in various platform-specific coding technologies. Instead, they can train their own developers in HTML5 programming and use those skills to develop mobile

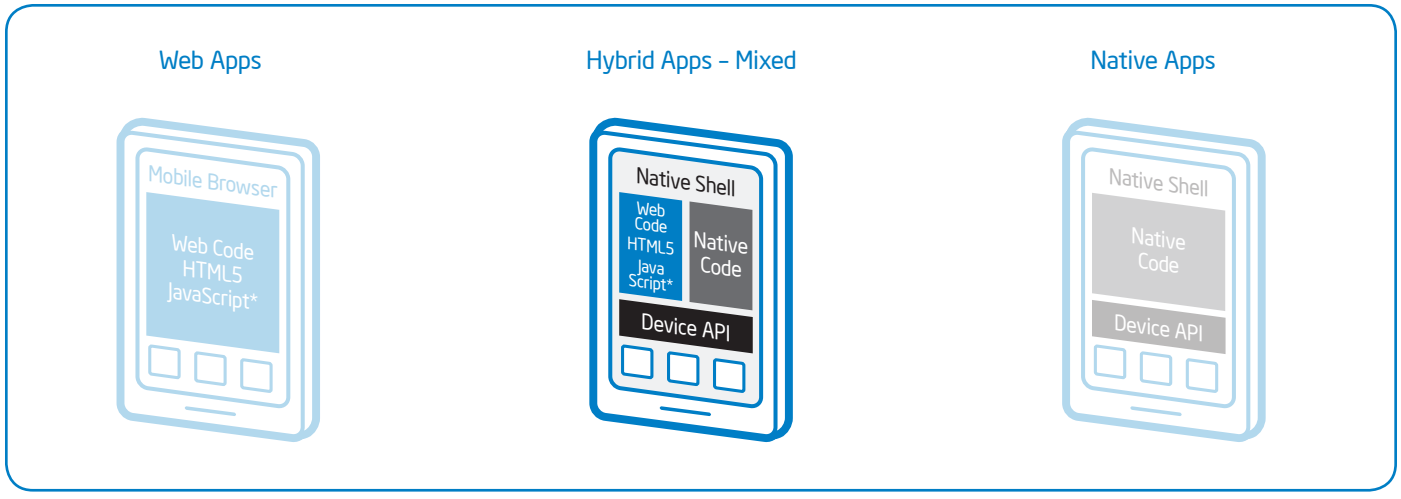

Figure 1. Of the three application delivery mechanisms considered during the definition of our mobile application development strategy, we chose a hybrid approach based on HTML5.

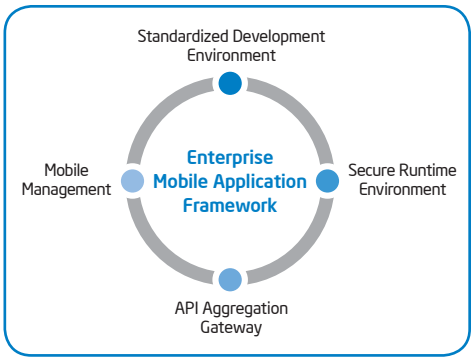

Figure 2. Our enterprise mobile application framework contains four primary components.

applications targeted at multiple platforms through our unique framework. Using HTML5 also simplifies the testing effort because some of the early testing can be done using standard desktop browsers that support HTML5. In this way we allow developers to concentrate on the UX rather than on enabling capabilities.

Framework Components

As shown in Figure 2, the framework includes four primary components: a standardized development environment, a secure runtime environment, an API aggregation gateway, and mobile management. The framework's standard environment allows developers to focus on application functionality and business logic. The framework handles other tasks through a "secure shell" in the device runtime environment.

We use several JavaScript*-based tools to separate logic layers and UI layers. This is an important approach because we build applications for specific device types but reuse the business logic. Each HTML5 application is "wrapped" with enterprise-specific logic. This approach helps standardize both the mobile application development experience and the UX experience. However, using the device API, developers can access device-specific capabilities, such as sensors, the Global Positioning System (GPS), and the camera, as well as middleware stacks such as the Intel® Context Decision Framework, Intel® Common Connectivity Framework, the Intel® Perceptual Computing SDK, and the Intel® Cloud Services Platform.

STANDARDIZED DEVELOPMENT ENVIRONMENT

Our goal is to make a standardized development environment available to developers of mobile applications at Intel. As shown in Figure 3, this environment provides all the building blocks developers need. It also enables developers to understand what enterprise back-end services they can access and how the application should interact with these services. The framework handles these interactions, such as data encryption, authentication and authorization, and device trust calculations.[3]

In addition to insulating application developers from back-end services such as security and authentication, the framework's mobile development environment simplifies infrastructure provisioning. Typically, when a project team wants to land a new application in the development environment, they must set up the appropriate infrastructure each time. The MADP aspect of the framework simplifies this process because a team has to set up the infrastructure only once; after that they can reuse the infrastructure for additional applications.

Using the framework, developers can create cross-platform applications that offer users single sign-on authentication, a consistent UX, and dynamic security as well as access to device-specific capabilities.

[3] See "Granular Trust Model Improves Enterprise Security," October 2012.

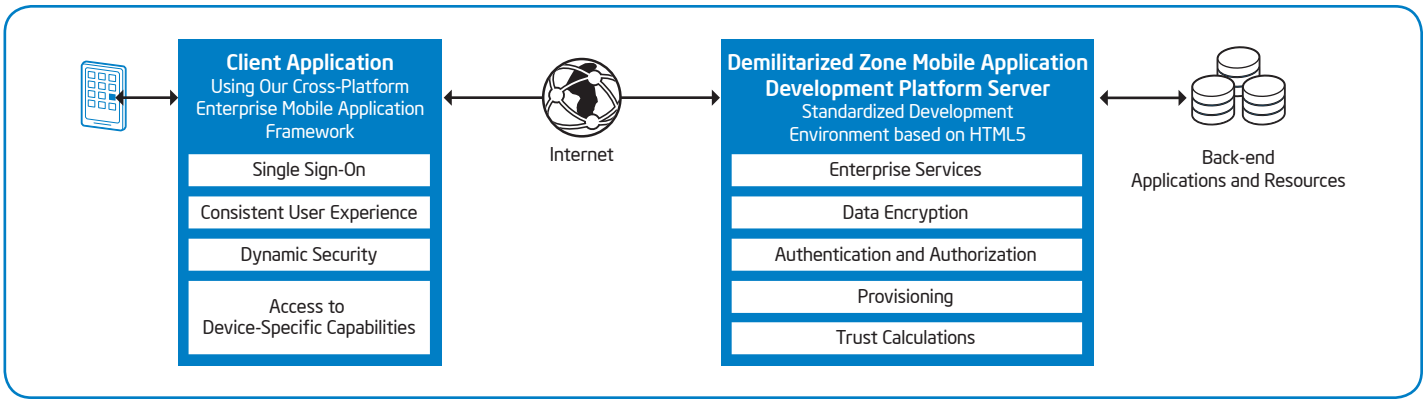

Figure 3. The framework's standardized development environment provides easy access to enterprise services.

SECURE RUNTIME ENVIRONMENT

As shown in Figure 4, the secure runtime environment combines security, rendering, and device adaptation using HTML5, CSS3, and JavaScript libraries. These components provide access to native system resources. When an end user launches a mobile application, the runtime environment's secure shell provides data protection at rest and in motion, encryption, and other security features. The secure shell handles the initial interactions with enterprise services, such as authentication, single sign-on, and provisioning. After these initial interactions are complete, the secure shell passes control to the mobile application to perform its function. If the application is running and needs to interact further with enterprise services, these services are also handled through the framework's secure shell.

The runtime environment is packaged with a mobile application to execute the commands on a mobile device. These can be HTML5 commands or native commands such as those used to communicate with the device's camera or GPS. Native commands are executed through a platform-agnostic open-source SDK, which forms a "bridge" to the device API.

The use of a secure-shell approach allows us to add another enterprise service to the developers' toolbox when new enterprise functionality is mature. For example, if we want to give developers access to location-based capabilities based on local sensors, we can expose these sensors through APIs or code libraries.

API AGGREGATION GATEWAY

At Intel, all connections to the enterprise network must be approved, and these approvals can take a significant amount of time to obtain. To simplify this process, we added a secondary middleware layer to our framework that abstracts APIs, such as those used to access back-end databases (see Figure 5). With the use of this API aggregation gateway, once a server is approved, many applications can use that server without additional time-consuming approvals. While not strictly necessary for mobile application development, having all APIs available through an API aggregation gateway makes it easier to control, maintain, reuse, and extend web services. The use of the secondary middleware layer does affect the performance for mobile applications. However, except in extreme cases of continuous requests for real-time data, the additional time is only a few milliseconds.

MOBILE MANAGEMENT

At Intel, mobile devices are either managed or unmanaged. A managed device can be personally owned or corporate owned, has certain minimum security features, and is managed by our mobile device management (MDM) system. Unmanaged devices are usually personally owned devices that have technical limitations or devices for which the user has chosen not to accept the IT polices, such as screen lock and encryption, that our MDM system enforces on the device.

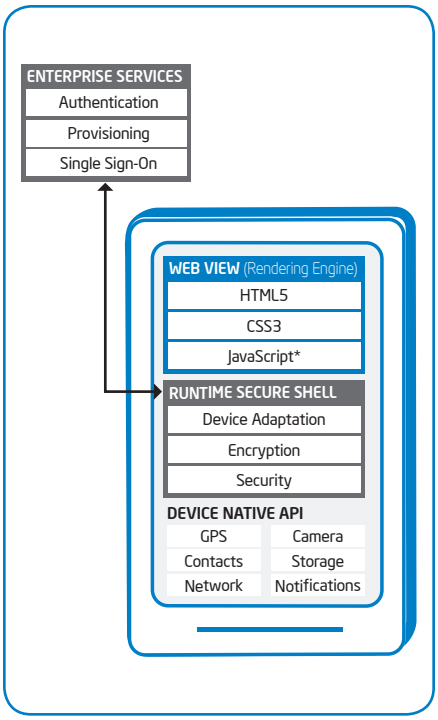

Figure 4. The runtime environment's secure shell handles enterprise service requests and can execute both HTML5 and native commands.

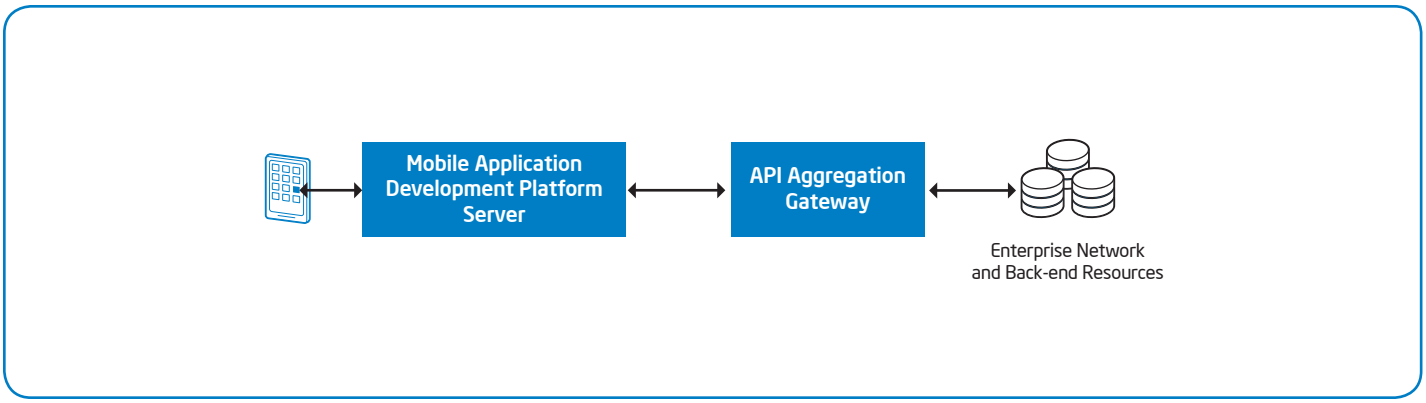

Figure 5. An API aggregation gateway enables reuse of back-end resources without the need for additional approvals.

As shown in Figure 6, our enterprise mobile application framework supports managed devices using MDM and a virtual private network (VPN). We are in the process of adding mobile application management (MAM) tools to the framework, which will allow the framework to be used for unmanaged devices. We are exploring the use of additional security capabilities in order to eliminate the VPN for managed devices.

We are also developing an enterprise application store, under the MAM domain, for applications on unmanaged devices. This approach enables us to provide better policy control and application lifecycle management.

The Mindset of "Secure to Enable"

We are in the process of integrating our granular security model with our enterprise mobile application framework.[4] Once the integration is complete, we will be able to modify the security access level for a particular device without having to re-engineer or rewrite applications. This ability will allow differentiated, trust-dependent functionality on different platforms. For example, a jailbroken device could have more limited functionality than a device with a high trust level.

From a security perspective, the runtime environment's secure shell is the "application" for which the trust level is calculated—the actual HTML5-based mobile application is contained within this shell. An integrated trust service will check trust at application launch, collect device and system attributes, initiate the trust calculation, and return the trust level. Only devices with an equal or greater trust level will be able to run that secure shell and, therefore, the mobile application contained in the shell.

Framework Benefits

Our enterprise mobile application framework provides benefits to all levels of the enterprise.

- **End user.** These benefits include device flexibility and UX consistency. As a user switches between devices to access the same application, such as from a smartphone to a tablet, the framework allows the UX to remain consistent and yet take advantage of the specific device's capabilities.
- **Application developer.** These benefits include reuse of UI controls, fast application development and deployment, and workflow capabilities that insulate developers from infrastructure provisioning and interface to back-end enterprise services. The framework provides information on all the necessary components needed to replicate the mobile application development environment. It also provides recommendations on the use of HTML5 for providing a customized and tailored UX across multiple devices.
- **Business group.** These benefits include efficient application development using HTML5 and reusable templates that are based on Intel business processes and aligned with business groups. For example, applications for Human Resources, supply chain, and social customer relationship management can all use the same template, making application development easier, faster, and more consistent.
- **Administrator.** These benefits include a unified security model across all device types, scalability for fast provisioning and revocation, flexibility to add new device types, and dynamic policy enforcement. By using a common framework to build and deploy several line-of-business mobile applications, we can lower development, sustaining, and infrastructure costs. Rather than hire a large number of developers skilled in separate mobile coding technologies, business groups now have the flexibility to use HTML5 developers to rapidly develop mobile applications that work across multiple form factors. With the planned integration of the dynamic trust-based security model, we will have the capability to dynamically change the security access level for an application without having to re-engineer or rewrite applications.

[4] For more information about Intel IT's granular security model, see "Granular Trust Model Improves Enterprise Security."

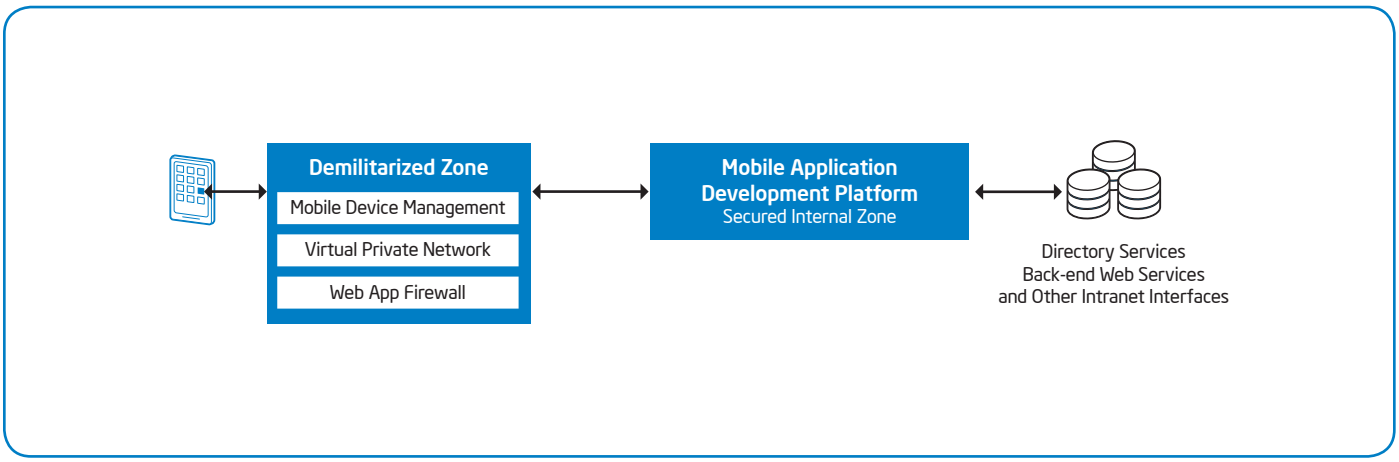

Figure 6. Currently, our enterprise mobile application framework supports managed devices using mobile device management and a virtual private network.

RESULTS

Our enterprise mobile application framework has been in development for the last year. We are developing the framework in stages, with additional features to be developed in future releases. We have developed and delivered two mobile applications using the enterprise mobile application framework; both these applications are now entering production pilot.

- Virtual Assistant. A set of functions and tasks that help Intel employee locate resources and information, such as colleagues and conference rooms, book audio bridges, schedule ad hoc meetings, and find navigation directions within a campus. This application targets all Intel employees with Apple iOS* and Google Android* mobile devices (currently over 35,000 users and growing).
- Design Assistant. A mobile application developed to increase design and software engineers' productivity. The Design Assistant enables engineers to remotely monitor batch jobs and take any necessary actions, such as suspend or restart. We plan to provide remote interfaces to other legacy applications, which will expand the functionality.

As shown in Figure 7, reusable infrastructure, approvals, and interfaces to enterprise services can speed application development significantly. Because we had to create the supporting infrastructure, get approvals, and configure the network, it took about four months to develop and deploy Virtual Assistant, the first application. Creating Design Assistant took significantly less time—only about two weeks—because all the infrastructure and back-end functionality existed, approvals were in place, and the network and firewalls were already configured.

In addition to substantially speeding up application deployment, the enterprise mobile application framework lessens the workload for the governance team because they can trust the framework and know that it can be used for secure application delivery. Application developers also benefit; development is easier and faster because the framework provides a common set of function libraries for security, authentication, the UI, and management. These aspects become reusable building blocks that do not have to be re-engineered for every application.

The framework uses HTML5 to provide convenient, pre-approved libraries and style sheets that are automatically applied to every application. The resulting standardized and harmonized UX can lower training requirements.

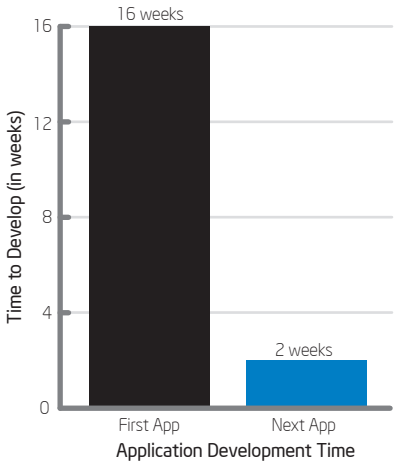

Figure 7. Reusable components and infrastructure can reduce application development time substantially, resulting in greater velocity and a faster time-to-market.

Transforming the IT Ecosystem to Support the Applications and Devices of the Future

Development of a cross-platform mobile development application platform is part of a larger effort by Intel IT to enable enterprise applications to support the devices of today, such as touch-enabled business Ultrabook™ devices and tablets, and also develop applications so they are ready for emerging interaction methods, such as voice, gesture, and perceptual computing.

We have identified five criteria that lead to a better end-user experience—security, ease of use, platform independence, device independence, and support for emerging devices and interactions. These same five criteria lead to a better application developer experience by removing obstacles and providing readily available tools to increase application developer productivity and efficiency.

Although the end result is applications that work better now and can take advantage of future technology changes, our work affects more than application development—it affects many components of the Intel computing environment, including security and privacy policies, mobile device management, mobile application lifecycle management, and application testing and scalability.

NEXT STEPS

Intel's computing environment is rapidly changing. We see Intel's client computing ecosystem increasingly using touch, voice, and other alternative perceptual computing-based input methods. In addition, Intel IT is actively exploring context-aware computing, which also has the potential to significantly enhance our mobile applications. Therefore, we are transforming our enterprise applications—and the supporting development infrastructure—to take advantage of these emerging capabilities.

We are laying the foundation for creating adaptive, next-generation applications that provide users with the information and tools they need at any particular point in time. Future applications may use cutting-edge interaction methods, such as eye scrolling, visual emotion detection, and voice-intonation detection in addition to other features such as augmented reality and anticipatory computing. Intel employees will be able to choose which input method is best for their particular situation and control which input methods they use. Applications will adhere to corporate guidelines about various input methods, to enable personal privacy at all times.

Different form factors offer varying amounts of screen real estate and different interaction methods. Our goal is to use our framework to design cross-platform mobile applications that can dynamically recognize which device and form factor is running the application, and respond appropriately by formatting itself to fit the available screen size. This approach will enhance the UX without increasing development costs.

We are also exploring combining MDM and MAM with secured mobile content management (MCM) and better mobile information and operations management. MCM is the availability of content synchronization capabilities combined with enterprise content management features for mobile device users. The key features of MCM will include the following:

- Powerful document management functionality that empowers smartphones and tablet users to directly edit, mark up, and organize nearly any form of content from their device of choice
- Real-time synchronization that allows users to access the most up-to-date and contextually relevant content
- Content sharing and mature content policy management, including role-, trust-, and context-based permissions that safeguard sensitive information
- Integration of the mobile content to collaborative and social systems of choice, with all the necessary forms of security and regulatory compliance

Mobile information and operations management includes application and session analytics, crash analysis and diagnostics, application and content versioning, device and application remote control for root cause analysis and correction, and application inventory. These features will be integrated with the capabilities of the corporate Information Technology Infrastructure Library.

CONCLUSION

Intel IT is developing a secure, cost-efficient, scalable framework that supports building, deploying, and sustaining mobile applications on various form factors. This framework lays the foundation for writing applications that can take advantage of future mobile technology, such as perceptual computing and context-aware computing.

Our enterprise mobile application framework, built on standard HTML5-based products, consists of a standardized developer environment, a secure runtime environment that provides access to back-end services as well as to device-specific capabilities, an API aggregation gateway, and mobile management. The environment provides building blocks that developers need to write applications, enabling them to focus on UX and business logic, instead of on back-end services. We are integrating Intel's granular trust model into the framework to provide differentiated, trust-dependent functionality.

Because our enterprise mobile application framework benefits end users, developers, business groups, and administrators, it has the potential to provide significant business value across the enterprise. For example, the framework can substantially reduce application development time. It took about 16 weeks to develop and deploy the first mobile application, Virtual Assistant. Because we reused the infrastructure and back-end functionality, approvals, and firewall and gateway configuration from the first

application, creating Design Assistant took only about two weeks.

Cross-platform development is crucial for success in the modern computing environment. We have found HTML5 to be an effective building block for robust, rich enterprise applications that have characteristics similar to both native applications and web-based applications. Using our framework, we can achieve a rich, consistent UX as well as rapid development of new applications.

RELATED INFORMATION

Visit www.intel.com/it to find white papers on related topics:

- "Building a Mobile Application Development Framework"
- "Creating Business Value through Context-Aware Computing"
- "Digital Personal Assistant for the Enterprise"
- "Granular Trust Model Improves Enterprise Security"

ACRONYMS

GPS	Global Positioning System
MADP	mobile application development platform
MAM	mobile application management
MCM	mobile content management
MDM	mobile device management
MEAP	mobile enterprise application platform
UX	user experience
VPN	virtual private network

For more information on Intel IT best practices, visit www.intel.com/it.