MOBILE APPLICATION SECURITY AND PIV DERIVED CREDENTIALS

NASA's Center for Internal Mobile Apps (CIMA)
Jane Maples and Peter Cauwels

August 26, 2015

CIMA
Center for Internal Mobile Apps

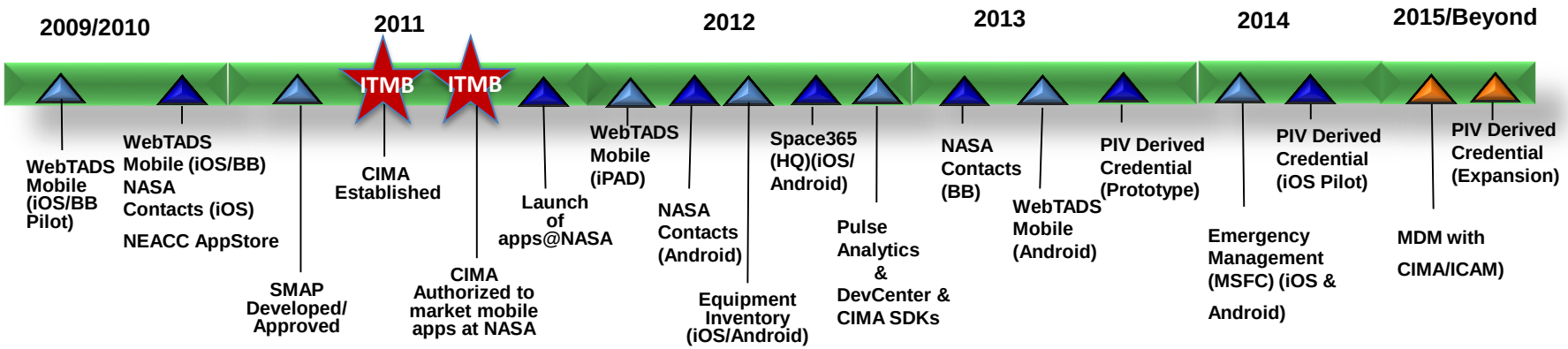
AGENDA

- CIMA Background
- CIMA Services
  - Hosting - apps@nasa
  - Mobile Development
  - Product Set
    - Pulse Analytics
    - Secure Mobile Access Point (SMAP)
- Mobile Authentication and Authorization
  - Derived Credentials
- Mobile Roadmap
- Questions

CIMA
Center for Internal Mobile Apps

CENTER FOR INTERNAL MOBILE APPLICATIONS (CIMA) BACKGROUND

- Our goal is to enable NASA's workforce access to the information they need, anytime, anywhere using CIMA's proven and secure architecture to deliver critical business functions directly to mobile devices

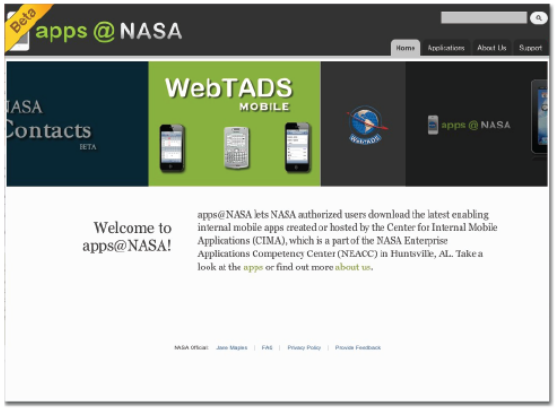


For Users...

Hosting and Delivery

One website (apps@NASA) for all NASA internal mobile applications

- Browse by category
- Rate and review applications
- Over-the-air installation and updates
- Search user forums for information and help



Multiple device platform support

- iPhone
- iPad
- Android
- BlackBerry

Easy installation to mobile devices with QR codes

https://apps.nasa.gov

Using a scanner application on the mobile device, users will be able to scan QR codes on documents or websites. The QR code will link to the install file for quick installation of the specific application or link directly to the apps@NASA website.

For Owners...

Analytics, Security and Branding

Analyze your Applications
Extensive metrics on all aspects of how users interact with your mobile applications

- Real-time application usage
- Analytic dashboard and ad-hoc reporting capabilities
- Customizable alerts and notifications for user events

Secure Your Applications
Full control on who can access and utilize your mobile applications

- Whitelist / Blacklist by users, groups, mobile device, etc.
- Remote application administration

Brand Your Applications
Provide a standard look and feel for all your mobile applications

- UX (User Experience) guidance
- Skinnable screen and widget templates
- Icon and graphics design

For Developers...

Pluggable Services and Cross Platform

Pluggable Services and Templates
Powerful plug-ins for accessing NASA services

- ICAM authentication and authorization plug-in
- Login and user preference templates
- Analytic and logging plug-ins
- Secure Mobile Access Point (SMAP) allows your app to reach protected NASA services and data

Cross-platform mobile application development services
Simple mobile solutions that span all major mobile devices

- Web application wrapper – deliver your web application as a native application
- Hybrid Web Applications – construct simple applications with HTML5, javascript and CSS
- MEAP – Mobile Enterprise Application Platform – construct powerful applications that access NASA services and data

Native mobile application development services
Feature rich native applications utilizing all of the mobile device's capabilities

- Full development life cycle support for iOS, Android and BlackBerry mobile applications
- Seamless integration with ICAM authentication and authorization services
- Secure access to NASA services and data

CIMA SERVICES

CIMA
Center for Internal Mobile Apps

CIMA MOBILE SERVICES

App Hosting

- NASA authenticated app hosting
- Full role and attribute based app provisioning
- Auto app updates via apps&nasa native app store

Product Set

- Web Wrapper
- Framework Module
- Pulse Analytics
- Content Management System(CMS)
- Secure Mobile Access Point (SMAP)

Development

- Native, hybrid, or responsive apps
- Objective-C, Swift, JAVA or responsive
- Backed by NEACC web services
- Deployable to apps@NASA store

Consulting

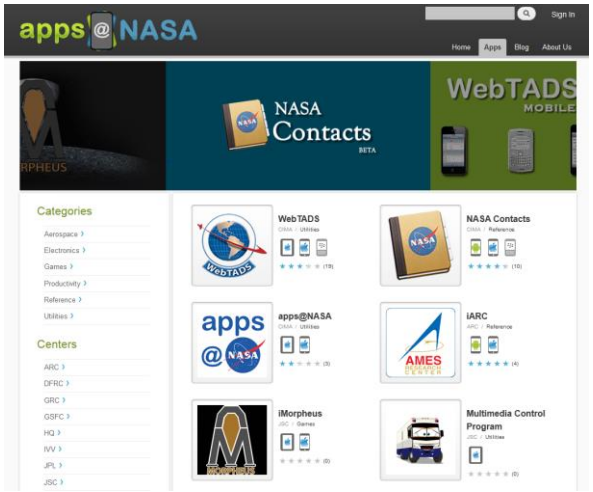
- Business Analysis and Requirements Definition Service
- Application Design & Marketing Service
- User Experience Design (UX) Service
- Application Testing Service

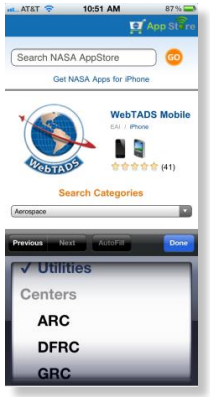
CIMA
Center for Internal Mobile Apps

APPS@NASA (WEB AND DEVICE)

apps@NASA (Web) is…

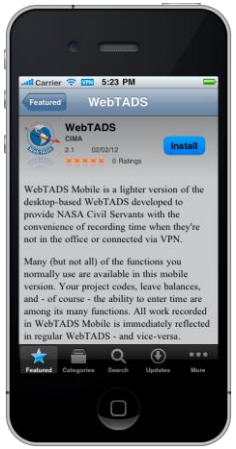
A website where NASA employees & contractors can download mobile apps that access NASA systems. These apps enable users to perform critical job functions at any time from anywhere, via Personal *AND* NASA mobile devices.





apps@NASA (Device) is…

A native iOS app where NASA employees & contractors can download mobile apps, receive updates and notifications.



CIMA
Center for Internal Mobile Apps

HOSTING

CIMA provides a platform for the development, management, and centralized distribution of NASA internal mobile applications. Internal mobile applications are those targeted only for NASA personnel, including contractors and credentialed affiliates.

The CIMA approach to centralization and distribution of NASA internal apps is Mobile Application Management (MAM). MAM is best characterized as application-centric. This approach makes it easier to target the things that matter most to NASA – the internal mobile apps and NASA data that may be used, and allows for the use of both Agency-issued and personal devices while user device preferences and personal private data are left alone.

Features of apps@NASA

- Agency level mobile application hosting and distribution for NASA internal mobile applications
- Multi-device support including iOS (iPhone & iPad), Android, and BlackBerry
- Rate and review applications
- Browse by category
- Search user forums for information and help
- Easy installation to mobile devices with QR codes
- Mobile development forum and code repository
- Hosting and distribution center for mobile applications

CIMA
Center for Internal Mobile Apps

CIMA MOBILE DEVELOPMENT AND DEVCENTER

- Software Library
  - Framework Libraries
  - Example applications
- Documentation Library
  - Getting started documents
  - Development standards
  - Technical instructions
  - Coding How-To's
- Instruction Videos
  - Getting started videos
- Development Forums
  - Development discussions

Downloads

iOS Framework 1.0
Developer library for iOS devices. It enables apps to use CIMA hosting, monitoring and deployment solutions.

Android Framework 1.0
Developer library and an example application for Android devices. It enables apps to use CIMA hosting, monitoring and deployment solutions.

iOS Example Application
iOS application showing how to use CIMA services.

Hybrid Plugin Example Application
Hybrid plugin example application description goes here.

Hybrid Pulse Example Application
Hybrid pulse example application description goes here.

Hybrid Example Application
Hybrid example application description goes here.

CIMA
Center for Internal Mobile Apps

PRODUCT SET

Our product set allows you to deliver your existing website as a mobile application, construct new mobile applications utilizing our secure infrastructure, and track usage. These capabilities are delivered through 4 components; CIMA mobile application web wrapper, framework module, user and application analytics/Pulse, and SMAP. In addition to these products CIMA also offers a Content Management System for mobile applications and websites, which eliminates the reliance on a second party for content management.

Features of our Web Wrapper Include

- Complete construction of a mobile application from an existing NASA web site or application
- Native skinnable login screen and simple PIN-based authentication with sites utilizing LaunchPad
- Allows users to access your website via the internet (if desired)

Features of our Framework Module Include

- Full support for iOS, Android and web (javascript)
- Provides native skinnable login screen and full integration with LaunchPad authentication
- Integrates seamlessly into all major IDE's (eclipse, Xcode, etc)

Features of Pulse Include

- Delivers real-time application usage
- Provides full transaction auditing and application logging through CIMA Insight
- Provides application alerting and event notification

CIMA
Center for Internal Mobile Apps

PRODUCT SET

Features of our Secure Mobile Access Point (SMAP) Include

- Secure mobile public access point for accessing protected NASA services and data
- Allows mobile devices outside of NASA locations to access protected NASA services and data
- Full whitelist/blacklist filtering by User, Device, Application, Application Version, Center

Features of our fixed price Content Management System (CMS) Include

- Push notifications
- Admin module accessible via the web and mobile device
- Central repository for documents, video, pictures
- File organization and version control
- Indexing, search and retrieval capabilities
- Pre-defined workflow
- Role-based content delivery
- Non-reliance on developers for content changes
- Relevant and current information
- Eliminates the need for end-users to download new versions to access new content
- Additional features/functionality, such as video may be purchased over the fixed price cost

CIMA
Center for Internal Mobile Apps

PULSE ANALYTICS

Pulse Analytics

- Mobile application owners

Pulse Insight

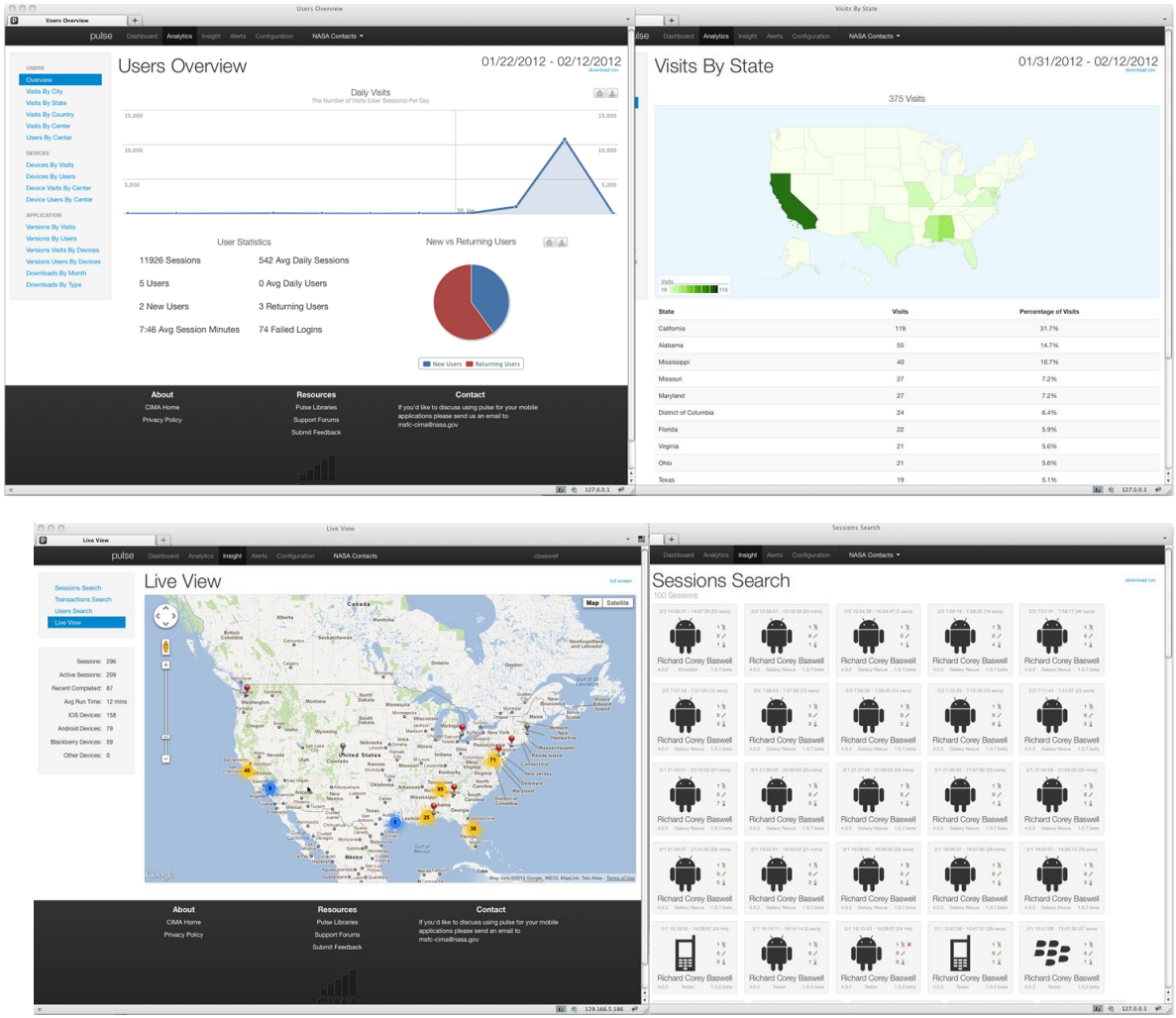
- Mobile application developers

Pulse Alerts

- Mobile application operations

Pulse Configuration

- Access Control Management

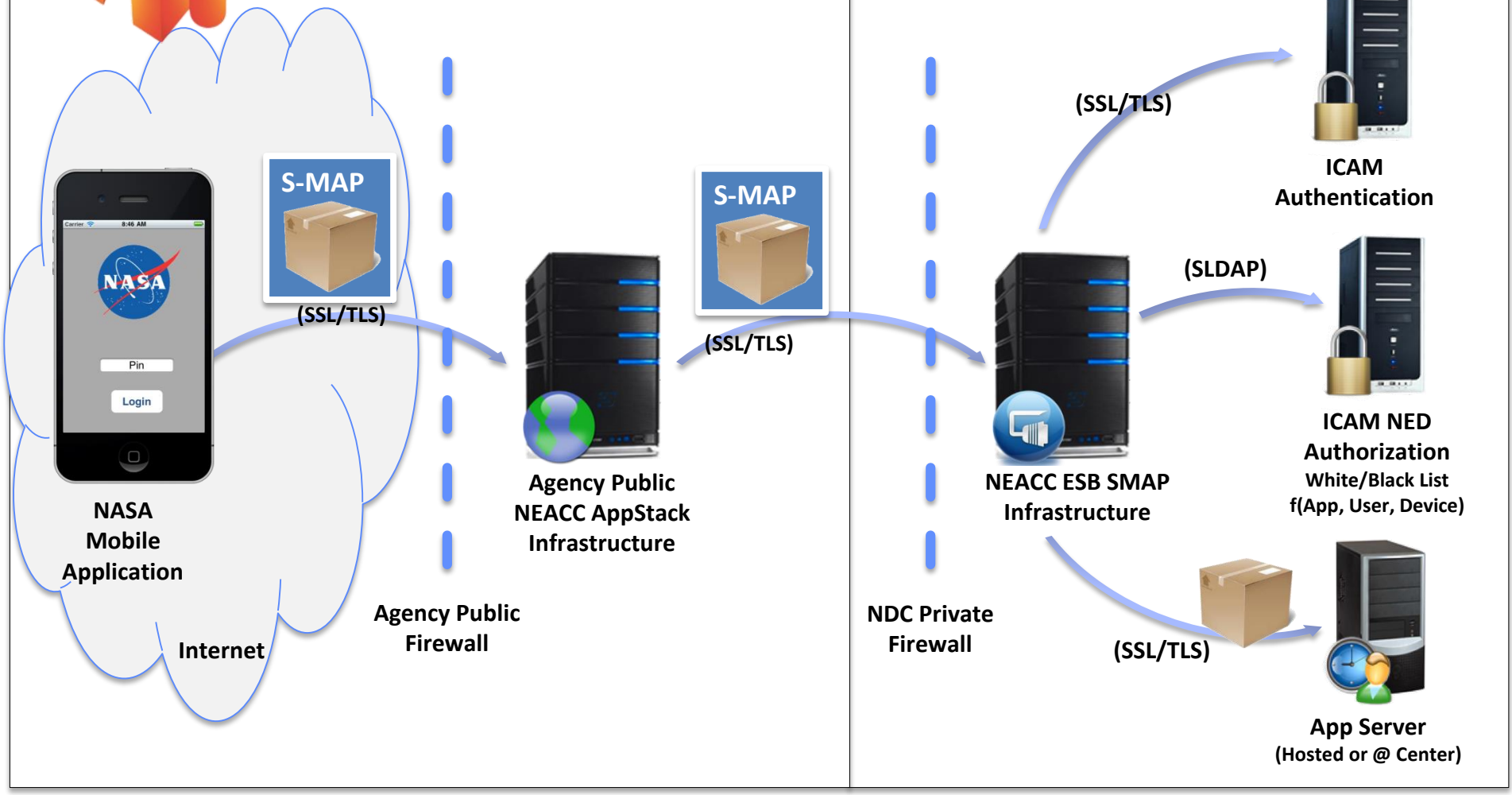


CIMA
Center for Internal Mobile Apps

CIMA – Secure Mobile Access Point (SMAP)

SECURE MOBILE ACCESS POINT

SMAP INFRASTRUCTURE



SMAP MESSAGING

Secure Access from Anywhere in the World

SMAP: Application ID, Login / Session Info, Metrics

URL: SomeService
Method: GET, POST, …
HTTP Headers: Content-Type, User-Agent, …
Message Body: The Request Data

SMAP

Private Web Server

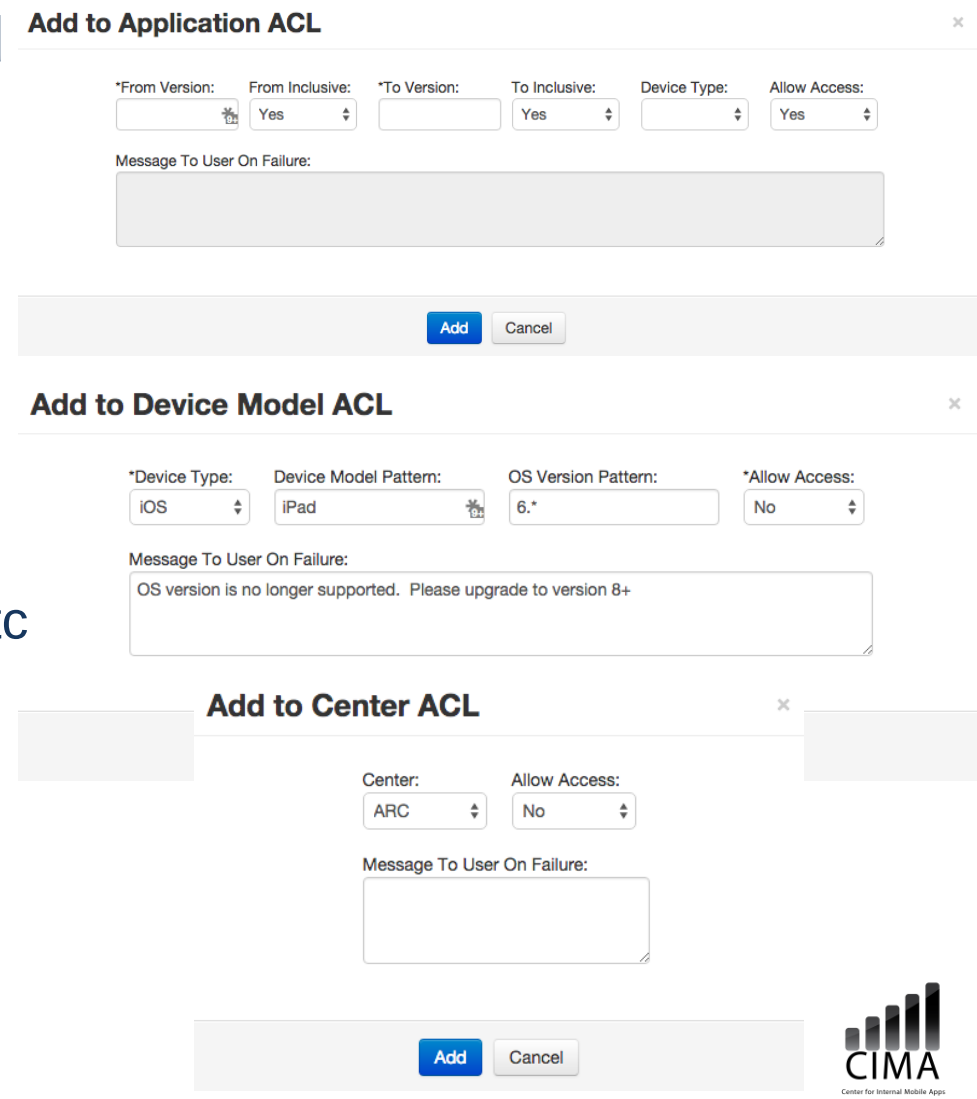
SMAP: Session Info, Configuration

Response: Code and message
HTTP Headers: Server, Last-Modified, …
Message Body: The Response Data

CIMA
Center for Internal Mobile Apps

SMAP ACCESS CONTROL

- Provides access to protected NASA assets
  - Data
  - Services
  - Systems
- Attribute Based Access Controls
  - User – type, center, etc
  - Device – model, OS version, etc
  - Application - version
  - Location
- Server side access controls for immediate response to security findings/incidents



Mobile Applications Authentication and Authorization

NASA (PIV) DERIVED CREDENTIAL ON IOS DEVICES

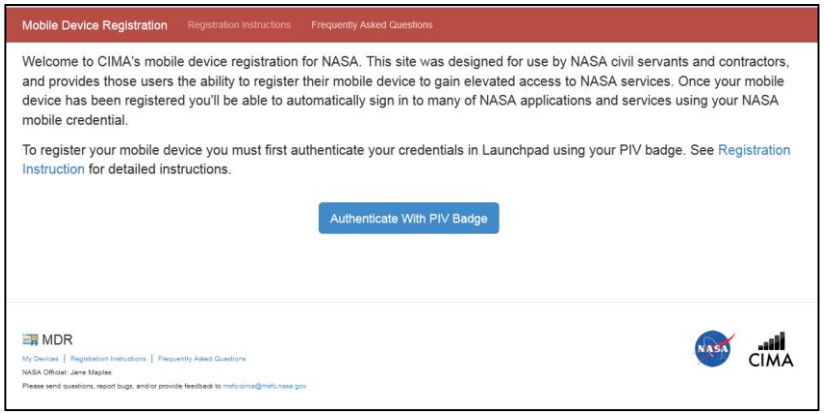
NASA (PIV) DERIVED CREDENTIAL OVERVIEW

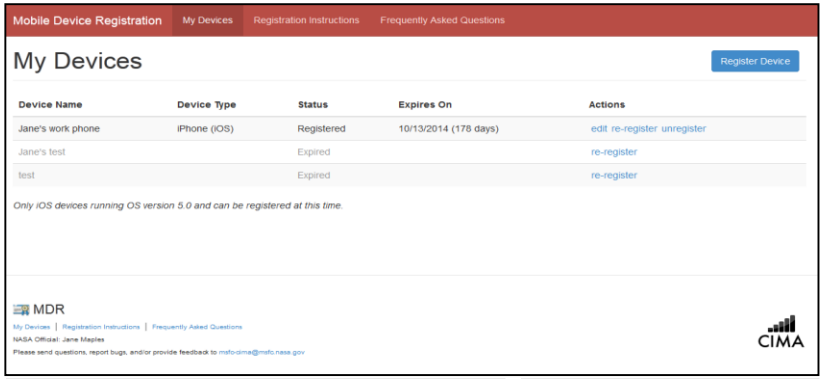
- Objective
  - Provide an enterprise solution for the implementation, utilization, and management of PIV derived credentials for mobile services utilizing Agency approved ICAM infrastructure and services.
- Scope
  - Derived from NASA PIV badge
  - Enterprise solution for the implementation, utilization, and management of PIV derived credentials for mobile services
  - Utilizes NASA approved ICAM infrastructure and services
  - Provides strong (LOA-3) user authentication on mobile devices
  - Soft certificate that lives on mobile device
  - Frees the user from relying upon additional components for securely accessing and utilizing NASA services on their mobile device(s)
- Use Case
  - PIV-derived authentication for CIMA enabled iOS mobile applications
- Agency Release occurred in the October 2014

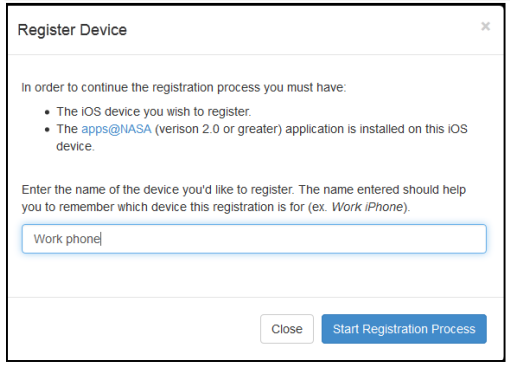
Recognized as ACT-IAC Igniting Innovation 2015 Awards Top 30 Finalist

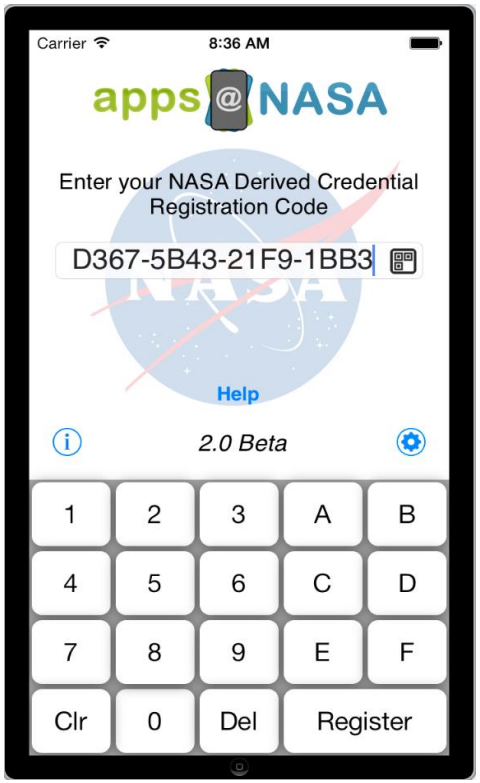
CIMA
Center for Internal Mobile Apps

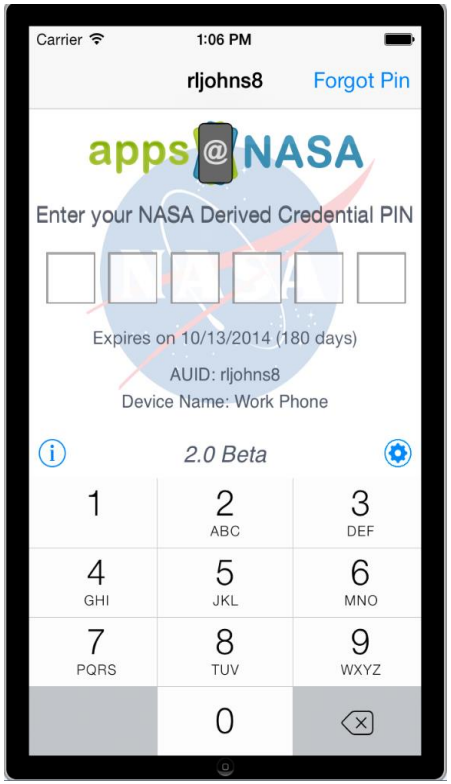
MOBILE DEVICE REGISTRATION (MDR)











CIMA
Center for Internal Mobile Apps

NASA (PIV) DERIVED CREDENTIAL PROCESS FLOW

2. Request Device Code

1. Login with Badge

4. Certificate Signing Request

(SSL/TLS)

3. Enter Device Code

(SSL/TLS)

5. Device/User Certificate

NASA (PIV) DERIVED CREDENTIAL PROCESS FLOW

1. *Login with Badge*
   - *User logs into any PIV Badge enabled computer.*
2. *Request Device Code*
   - *User launches Mobile Device Registration (MDR) website (browser-based)*
   - *PIV Authentication occurs*
   - *User requests device code*
3. *Enter Device Code on Mobile Device NASA Apps (MAM) application*
   - *User enters device code from MDR website*

4. *Certificate Signing Request (CSR)*
   - *Public/Private key generated on device*
   - *Device Code and CSR are sent to CIMA/ICAM*
5. *Device/User Certificate*
   - *ICAM service generates Device/User Certificate*
   - *Certificate sent and stored on Device*
   - *User secures private key for Certificate with PIN (6 char)*

Mobile Device Management (MDM)

- Certificate Lifecycle Management (CLM)
- Application Lifecycle Management

Shared Service Possibilities

MOBILE ROADMAP

CIMA
Center for Internal Mobile Apps

NASA'S MOBILE ROADMAP

MDM Implementation

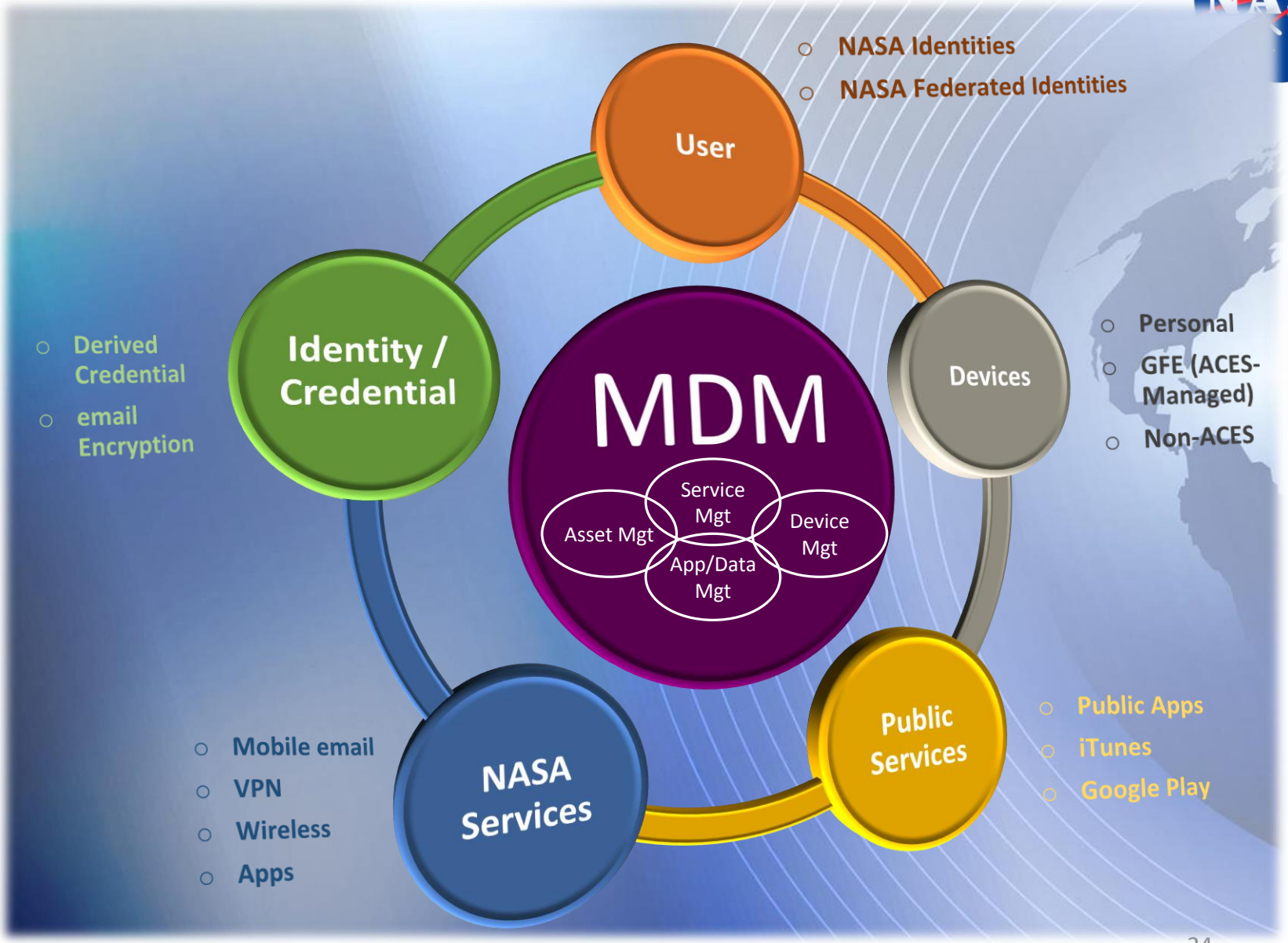
- Certificate Lifecycle Management (CLM)
  - Secure and Manage the user's identity
    - Implement and manage the lifecycle of strong credentials
    - Implement and manage encrypted email
    - Provide strong authentication for mobile services
- Application Lifecycle Management
  - Secure and Manage the mobile applications and services
    - Implement secure application container for NASA services
    - Implement application provisioning and lifecycle management of applications

Other Items

- NASA Internal Possibilities
  - Incorporate the Volume Purchase Program (Apple) into the apps@NASA offerings
  - Consolidate Public App Management and Internal App Management with one organization
- Shared Services Possibilities
  - CIMA Mobile application management services (lightweight MDM) shared service provider
  - CIMA 'app hosting' shared service provider
    - Web based user self-service appstore
    - Native mobile appstore clients (iOS, Android)

CIMA
Center for Internal Mobile Apps

MDM PROJECT SYSTEM CONCEPT



CIMA
Center for Internal Mobile Apps

CERTIFICATE LIFECYCLE MANAGEMENT (CLM)

- MDM CLM integration enables the certificate lifecycle management capability for the following credentials
  - email Encryption (S/MIME) Credential
  - email authentication using the Personal Identity Verification (PIV) Derived Credential
  - Launchpad Websites authentication using the PIV Derived Credential
  - Wireless 802.1X Wi-Fi authentication using the PIV Derived Credential

Contact us at: msfc-cima@mail.nasa.gov

QUESTIONS

CIMA
Center for Internal Mobile Apps

BACK-UP

CIMA
Center for Internal Mobile Apps

Mobile Enterprise Application Platform (MEAP)

CIMA MEAP OVERVIEW

CIMA
Center for Internal Mobile Apps

CIMA MOBILE ENTERPRISE APPLICATION PLATFORM (MEAP)

Enterprise Connectors
Technical Adapters and Protocol Support

SMAP
Secure Mobile Access Point
Access Control

LaunchPad (Open SSO)
Authentication

Native Mobile Apps
Apple, Android

Message Bus
Event Processing and Routing

Pulse
User / Device Metrics
Auditing / Logging

NED
NASA Enterprise Dir
Authorization

Mobile Websites
Mobile Web

SOA
Web Services
REST
SOAP

APPS@NASA
NASA Enterprise AppStore

idMAX
Account Provisioning

Hybrid Mobile Apps
Cross Mobile

ESB

AppStack

ICAM Services

IDE Tooling (Development)

CIMA Mobile Enterprise Application Platform (MEAP)

CIMA
Center for Internal Mobile Apps