Identity Management and Biometrics
- laying the foundation for solution applications

4th WCO Technology and Innovation Forum
Argentina - Nov 2013

www.technobrainwestblue.com

© 2013 Techno Brain West Blue
Current challenges before Customs Administrations

- How do we control the cost of operations?
- How can we provide better value to our users and stakeholders?
- How can we electronically manage our employee data?
- How can we coordinate all our applications – existing and new?
- How do we provide access to our applications to our employees – field and office?
- What IT innovations can we deploy that are sustainable?

Need of the hour.....
Current trend in enterprise mobility

- Over Half of businesses are making line-of-business apps accessible from mobile devices.
- 73 percent of businesses rated "increased efficiency" as a very important key benefit of mobile computing.
- Half of employees use tablets for both business and personal use.
- Half of employers expect to invest in an MDM solution this year.
- Half of Info workers use three or more devices.
- 60% of devices reported by Info workers are used for work and personal purposes.
- 90% of Fortune 500 are deploying or testing the iPad.
- 830m enterprise smartphone and tablet app users by 2012.
Outlook of Customs Administrations for a mobile platform

- Improve quality of information to and from the field
- Improve Responsiveness
- Reduction in administration times
- Improve accuracy and quality of reporting
- Meet and beat SLA’s
- Improve user satisfaction
- Reduce the need for paperwork and manual intervention

Enable mobility across the organisation

- Have short ROI – reduce risk
- Integrate with back-office systems
- Robust security mechanism
- Instant deployment
- Be flexible and adaptable
- Improve quality of information to and from the field
- Improve Responsiveness
- Reduction in administration times
- Improve accuracy and quality of reporting
- Meet and beat SLA’s
- Improve user satisfaction
- Reduce the need for paperwork and manual intervention
THE PROPOSED SOLUTION

- A comprehensive android tablet-based mobile security framework to enhance and extend the e-Services currently offered by Customs Administrations

- A solution that will enable Customs officers and relevant stakeholders to carry on their assigned tasks in the field and be able to securely conduct and post transactions through secure channels in real-time.

The system will serve Customs Administration in reducing inappropriate use of their services, reduce fraud in transactions, and enhance information sharing across various platforms and departments and increase revenue collection.
Multiple Applications – Single Device – Single Sign On

- As part of the implementation, all current officers of the Administration may be enrolled and registered in the system
- New officers will be enrolled on joining the service and exiting officers deregistered - **Centrally**
- Change in roles / assignments / departments will be effected within the system without having to re-enroll the person or recall the person to base

...supporting the Single Window Concept
Device capabilities:

- 2 Cameras – Front facing 2MP and Rear facing 4MP
  - Autofocus camera with flash for 2D/3D barcode reading
- Video
  - 1080p, mini-HDMI
- Mobile Phone
- 3G/2G data connectivity for mobile situations
- Certified Embedded Secure Element
  - Tamper resistant
- Large Area fingerprint sensor
  - Good quality image for biometric verification
- ISO 14443 NFC Reader integrated
- Large capacity 6000 mAh battery
  - 1 day usage guarantee, based on a standard scenario
Device capabilities: Easy browser-based device tracking and administration

Monitoring agencies / Head offices can in real-time access information being gathered by field / emergency response personnel and render the data on to a map for better analysis and forward planning.
The Bio Lock is an innovative solution provided by Techno Brain – West Blue that restricts the usage of the mobile device to its unique user. The solution is fully integrated as part of the Android System and is based on the mobile device hardware secure components.

- **User Biometric credential stored into Secure Element**
  - EAL4+, EMVCo and CAST Certified

- **Biometric Enrollment only by an Administrator**
  - The user cannot grant another user and/or lend the device
Device capabilities: Secure Administration

The Secure Administration Solution provided by Techno Brain West Blue integrates into the Android System for high security. Access and usage of the device is fully controlled by an application running from within the Secure Element.

- Biometrics and/or Certificates stored into NFC Secure Tag
  - High security multi factor authentication
- Administrative rights controlled by Secure Element
  - Payment terminal operating model
Uniqueness of the proposed solution

- Full control on the device hardware and software
  - Secure elements and Secure Domain
  - Android Kernel, Android Operating System
    - OS customizable for an enhanced security

- Full control during device production
  - Pre-Personalization of secure elements
  - Customization of the device with logos...

- Integrated solution
  - Integrated Fingerprint sensor with mutual authentication sensor/tablet: impossible to replace the fingerprint sensor by a fake one.
  - Embedded Secure Element EAL4+ certified
    - for cryptographic key storage and high security Biometric Match on Card
  - NFC reader ISO 14443 compliant
2 STEP IMPLEMENTATION PROCESS

**Step 1:**

- Enroll all Officers using *SecuRegister*, Techno Brain West Blue’s flagship identity management framework.
- During this step, the demographic details of the Officers, including 10-fingerprints, photograph, signature etc. will be captured and stored in a secure database.
- Each record will be searched and verified against duplicate entries to ensure only unique records are stored in the secure database.
**Step 2:**

- Once Officers are registered in a secure database, credentials of individual Officers are attached to designated unique devices on the android-tablet
  - This process will involve transferring the credentials (fingerprint templates and other necessary biographic details) to the android-device
  - This secure information will be securely embedded into the fool-proof “embedded hardware secure element” of the android-tablet using a custom-built interface
  - This entire process is done only by authorized, security cleared personnel only
- Once a credential of an Officer has been successfully embedded into the android-device – the Device ID (unique to each device) is then tagged against the Officer’s record in the secure database
- Only the designated officer will be able to log-in securely (using fingerprint-based credentials) into the device
  - no need for connectivity to the secure database for authentication purposes as all fingerprint templates are stored locally
  - All authentication during power-on and unlocking will happen locally
- The device is now ready to be loaded with any secure transaction application
Usage Life Cycle

- **Pre-Personalization**
  - At the factory, all the devices are pre-personalized with the Customs Administration’s specific Secure Domain, and certificates are loaded using a secure Global Platform process. No one else will be able to access the information stored into it.
  - Other credentials are also loaded into the secure element that will identify the hardware during the complete lifetime of the Tablet.

- **Biometric Enrollment Step**
  - Using the SecuRegister application, the officer biometric credentials are captured and stored into a dedicated database. Biometric template should be stored into ISO/IEC 19794-2 Finger Minutiae Format.

- **Personalization**
  - The personalization step is an important step for the security of the process. It deals with the adaptation of a specific device to a specific Officer so that he/she will be the only one able to unlock the device for its utilization.
  - This personalization is done under the supervision of an Administrator that can:
    - Verify the identity of the Officer
    - Authorize the transfer of the credentials into the Tablet Secure Element using his/her Administration credential.
  - Once the personalization done, only the right Custom Officer can unlock the Tablet.
Usage Life Cycle

- **Device usage**
  - After all these steps of configuration, the device is ready to be used for its application.
  - In the field, the device may need to send pieces of data to distant server. For instance, each time the tablet is unlocked, the Officer ID and the Tablet ID are logged into a database. Access to these distant services will be authorized only to devices that are allowed. The authentication is based on the internal secure element.

- **Changing users**
  - Users may be deregistered from the system instantly and centrally, rendering the tablet useless.
  - For any reason, if a device needs to be assigned to another user, it can only be done by an Administrator using his personal smartcard.
  - Only an Administrator can unlock a Device.
Usage Scenarios

- Deployment of any number of custom-built applications to extend the reach of existing applications
- The roles and rights of enrolled officers can be suitably modified to align with new designations and responsibilities
- The mobile device can be securely offered for external actors including Customs Licensed Agents, Freight Forwarders etc.
  - Thereby increasing the control that Customs can exert on their deployed systems
  - Providing increased flexibility in interacting with the Administration’s secure systems
- Extending the secure device on to external Customs actors may act as a revenue stream (pay-per-usage or leased model) which can self fund and sustain the project as a whole
SOLUTION BENEFITS

- **Secure mobile channel:**
  - Using embedded device level security mechanisms, the system will offer a biometric-based security solution for the Customs Administration

- **Enhanced Productivity:**
  - By extending the reach of current and future e-Services, the system will enable Officers to enhance their productivity and decrease the time taken for processing transactions in line with trade facilitation goals

- **Enhanced Accountability:**
  - As a result of the secure biometric-based access, management will have greater and fool-proof control and visibility of all transactions being conducted by their Officers (field and office) whilst increasing the turn-around-time of processing these transactions.

- **Enhanced Decision support and Reporting:**
  - The proposed solution will ensure that all the information necessary and pertaining to a transaction is available to officers on a need to know basis and in real-time, enabling quick informed decisions.
  - Further, since the communication is secured using biometric-data of the officer, the system provides a fool-proof mechanisms in auditing and reporting to management.
Valentina Mintah
Director, Techno Brain West Blue Ltd
valentina@technobrainwestblue.com

Thank You