



This photo was taken by Adventier consultant Luke Finsaas at the legendary site, Poon Hill.

**ENJOY THE
FREEDOM.
SECURELY.**

MOBILE SOLUTIONS

THE TREND

Have you noticed the trend? Mobile devices are becoming more pivotal to your critical business processes. You are approving the project's next step, reporting on a crucial sales meeting, and reviewing financial reports as you flag a taxi. Mobile devices are pioneering new forms of productivity. Now you can do business, no matter where you are or what you're doing.

LEVERAGE MOBILE INVESTMENT

Our solutions allow you to fully leverage your investment in mobile technology. Issue one-time log-on passwords. Authorize employees to run transactions. Create a phone application for system password self-service. With the correct security architecture in place, your employees can do their business from Hong Kong, Dubai or the breakfast table.

NEW SOLUTIONS, OLD PROBLEMS

Mobile devices offer new solutions for old problems. For instance, employees write down passwords and leave them in the open. By issuing one-time passwords through mobile devices, you eliminate compliance risks with strong, convenient two-factor authentication. Reduce service desk requests by giving users a way to reset their own passwords through their mobile devices.

SECURING MOBILE DEVICES

Mobile devices also expose your enterprise to new risk. Our solution allows you to control your company's mobile devices from a central cockpit. Wipe lost phones, encrypt data, build roles, roll out security policy, and monitor or even block risky interfaces. All communication is protected and keys are stored safely on each device.

SOLUTION SCENARIOS

- Deliver one-time passwords
- Enable Password Self-Service
- Realize mobile Single Sign On
- Control mobile devices from a single cockpit
- Ensure device configuration security with Mobile Firewall
- Use certificates to secure all communication between device and in-house server
- Control device functionality by location through GPS with Location Based Service

ABOUT ADVENTIER

Adventier offers innovative solutions for Enterprise Applications Security and change management.

MOBILE SOLUTIONS

SECURING MOBILE DEVICES

With our Mobile Suite, you can achieve complete control over your mobile devices. You will save cost and time configuring devices; optimize security; enable scalability; and turn your current mobile strategy into a longterm success. We set a new standard in management and administration of mobile devices.

MOBILE ENTERPRISE

Mobile Enterprise efficiently manages mobile users, rights and roles, as well as the integration of mobile users in the existing infrastructure.

LDAP, CA AND TRUST CENTERS

For complex domain structures, there are interfaces for LDAP directories that allow easy integration of mobile users from the in-house directories. Certificates may be issued via your own Certificate Authority (CA) or you can optionally integrate an existing CA or Trust Center.

ROLL-OUT

Automatically configure and secure the installation of devices with Mobile Enterprise. Third-party software may be installed directly on the end device. Certificate distribution can be done via Over-the-Air, Web Portal, or ActiveSync.

NEW DEVICES WITHOUT CODE CHANGE

Embedded systems are highly hardware dependent. We meet the surge of new devices with a unique, independent database, which enables you to support new devices without code changes.

BACKUP & RECOVERY

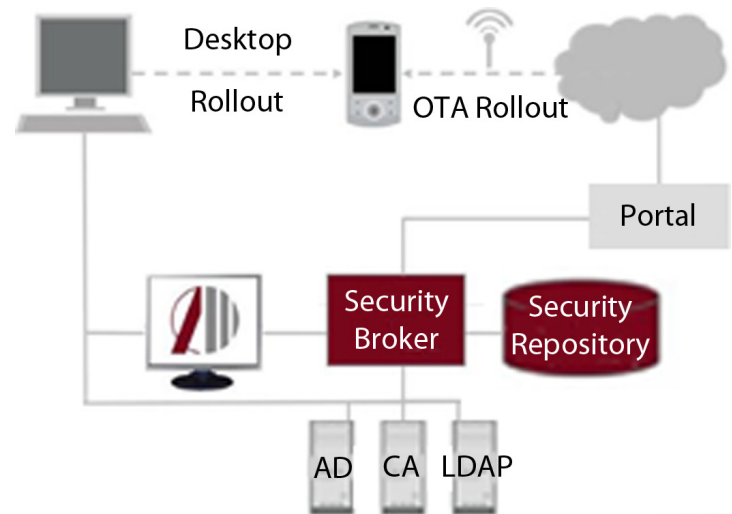
After the roll-out, an automatic backup of device configuration and installed certificates allows for immediate use of the device in case of a hard reset.

MOBILE FIREWALL

The Mobile Firewall protects the configuration of your mobile devices and, at the same time, blocks and monitors risky interfaces.

CONNECTIVITY

Use of WLAN, Bluetooth and Infrared adapters need explicit authorization from the firewall settings, thus avoiding the risk of Always-On radio technologies for wireless interfaces.



Mobile Enterprise structure

USER RIGHTS

The Mobile Firewall allows an administrator to grant access rights for settings modification. Rights for installing, editing and manipulating for modems, Proxy Server, VPN-connections, email accounts, etc. have to be explicitly granted by the administrator.

USB ACTIVE SYNC

The Mobile Firewall also controls the local Active Sync connection to Desktop PC and Notebooks. IT-administrators specify which mobile devices are authorized to exchange, update or copy data (e.g. e-mails, contacts) with which Desktop PCs.

MOBILE FEATURES

Mobile Firewall prevents use of unwanted applications. Via positive or negative lists, administrators define which programs will be executed and which features are allowed to be used (e.g., program requests, network accesses, built-in digital cameras or SD cards).

MOBILE SOLUTIONS

SECURING MOBILE DEVICES (CONT.)

MOBILE AUTHENTICATION

MOBILE PKI

Mobile PKI is the safe and easy certificate solution for mobile devices. Roll-Out and certificate management are completely automated. Mobile PKI uses X.509 certificates of a Public Key Infrastructure to secure all communication (i.e. email, calendar) between the device and the in-house BlackBerry Enterprise Server.

TWO-FACTOR AUTHENTICATION

Different applications and users need different authentication methods. Our mobile suite administrates the certificates and private keys in a secured key store. By binding the key store (username/password) to the device ID and/or the SIM card (security token), a multiple-factor authentication may be realized.

LBS AUTOMATION

LBS Automation adds location based services to the mobile suite. On basis of geo positioning data, the location dependent behavior of the mobile device is automated. It uses the XML-Standard Keyhole Markup Language (KML) and offers interfaces for import and export of geo data.

LOCATION BASED CONFIGURATION

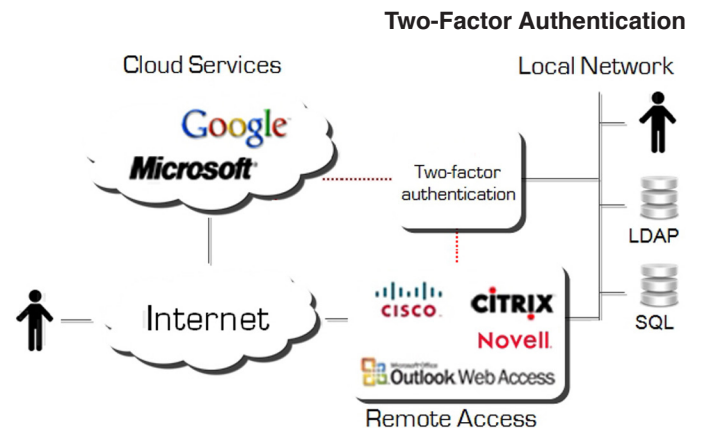
Profiles containing settings for configuration are assigned to locations and zones and the device uses the rules at entering/leaving a zone. An automatic reconfiguration is possible as well as changing of security settings and user rights.

LOCATION BASED ACTIONS

Upon entering a zone, additional free definable actions may be accomplished. For example, the user files may be opened automatically, applications started or a video file played with information regarding his user's location.

GPS & GSM

GPS Data and/or GSM cell information can be used for position determination. This data is checked and processed in configurable intervals.



LEVERAGING MOBILE DEVICES

ONE-TIME PASSWORD (OTP) SERVICE

Our One Time Password Server secures access to applications and systems with strong, multi-factor authentication. Easily integrating into your existing environment, this solution fully supports most remote access solutions, making installation a breeze - you'll be up and running in no time. With one single application, you'll be able to support multiple authentication methods, including: OTP sent via SMS, X.509 certificate, pre-generated OTP, physical token, and OTP sent via e-mail or instant messaging.

PASSWORD KIOSK

The research is startling. Approximately 50% of all help desk calls are for password resets, and the average help desk labor cost for a single password reset is about \$22 (Gartner). With the Password Kiosk, users can easily and securely self-administer their personal details and reset or change their password. Password Kiosk also provides monitoring and reporting facilities.

There are several different methods for verifying a user's identity in a password change. Leveraging your mobile investment, you can send a one-time password to your user's mobile device. You can also use secret questions or if there is a PKI infrastructure in place, a user certificate can be used to identify the user.

All operating systems with Java Virtual Machine (JVM) Version 1.6 or higher are supported. Supported user databases include LDAP v3 compliant directory service (Microsoft Active Directory, Novell eDirectory, Sun Java System Directory Server, Siemens® DirX*, OpenLDAP...).