

2011-09-26

A **WIP** WHITE PAPER



Secure Application Framework (SAF)

Contents

Table of Contents

Introduction.....	2
Problem Statement.....	2
Previous Options.....	3
SAF Solution.....	4
SAF Benefits.....	4
Implementation.....	6
Summary.....	6

Introduction

In this paper WIP will present a new concept called app management, which allows companies to capitalize on the opportunities to increase productivity afforded by employees bringing their own devices to work whilst addressing the security issues this raises.

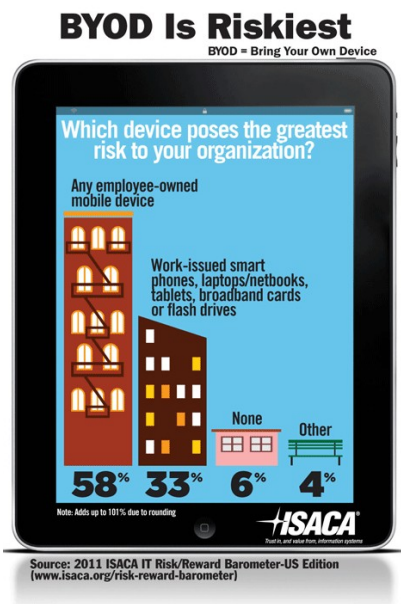
Problem Statement

More and more people invest in private smartphones and due to this increasing use of connected devices, employees start bringing these devices to work. The employee wants to increase productivity and become more efficient by using their new device but switching between private and work devices is inconvenient and could be counter-productive. Employees want to have both private and work-related information at hand all the time in the same device. Often the privately bought device is more modern and capable than the corporate model of choice.

These private devices are hard or impossible for IT departments to control. Many companies are now preparing for this trend and creating strategies and policies for BYO (BringYourOwn) scenarios.

Private devices also include devices provided by the company, which are also allowed to be used for private purposes.

ISACA's 2011 IT Risk/Reward Barometer results clearly shows that the greatest risk companies see is BYOD (BringYourOwnDevice).



In a large corporation there are likely many employees who, on their own, develop work-related mobile applications specific to their department needs. These applications, which could be a big asset, can also become a security breach in the corporate computer environment if not secured.

This needs to be addressed because Gartner predicts *“By 2014, 90 percent of organizations will support corporate applications on personal devices.”*

Previous Options

The solution to the threats from BYO is traditionally to simply forbid usage of private phones and devices in the corporate environment. As often stated by system administrators: *“If we can't control it, we won't support it.”*

These constraints can in fact have a negative impact on security when employees start circumventing them using external network storage and solutions to still be able to use their private devices. Frequently encountered workarounds are to forward sensitive information to external third-parties such as Hotmail and Dropbox.

Traditional MDM-systems (Mobile Device Management) can lock down a device to only allow access to certain applications or information.

The downside of MDM lockdown:

- only a short list of devices can be supported
- productivity and freedom are restricted
- maintenance and support costs increase
- does not address allowing a private device in a corporate environment

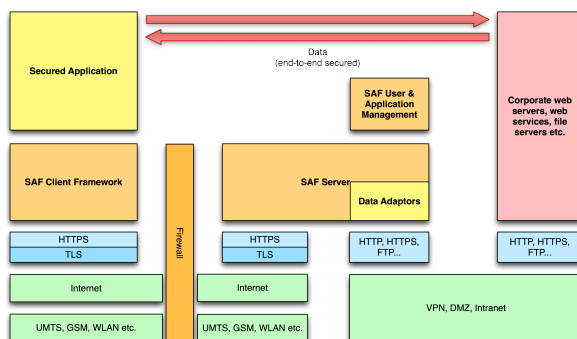
The solution is called app management, a concept that enables access to resources in a controlled way and where applications, data, devices and users can be easily managed.

SAF Solution

SAF (SecureApplicationFramework) from WIP is app management and solves this puzzle. SAF helps taking the first step on the path of your vision – zero administration cost.

The SAF server is placed in the DMZ of the company and can control remote access to corporate resources such as documents and other intranet resources. SAF can be combined with existing MDM and anti-virus solutions. Clients can be either iOS or Android devices.

When an application is built using SAF you can control access to resources when the user is logged in to the application and not when the device is merely unlocked.



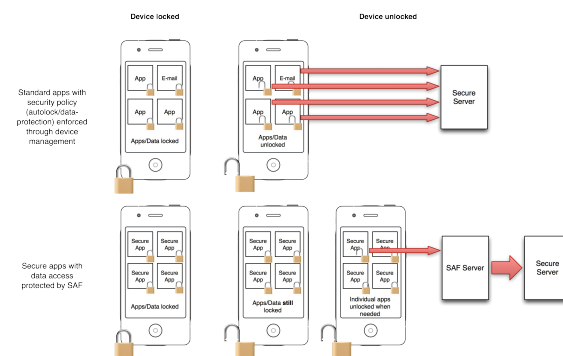
SAF handles the entire authentication and authorization process as well as provisioning of new mobile users and applications. SAF have support for a large range of authentication methods including static PIN, challenge/response, OTP, RSA SecureID and pattern. It also handles all communication and storage.

The framework allows companies to build their own secure native corporate clients.

SAF Benefits

Data-leakage Prevention

Without SAF, data might unintentionally fall into unauthorized hands since normally a device is locked by PIN-code and when the device is unlocked all information and applications on the device are open and accessible. When using a mobile application built using the SAF framework the information is only available when explicitly unlocked.



This means that even when the device is open and unlocked, the data is safe and unavailable until an authorized user opens it. Data includes e.g. corporate email and document storage.

Private App Store

Adding a user and allowing private devices in the corporate infrastructure is easy with the SAF framework. The SAF solution includes a user- and device provisioning portal where you can deploy applications and give users access to the application and its contents.

The installer is pushed out to users' registered emails or phone numbers. The applications and application updates are handled by the SAF server on corporate premises instead of by public stores such as iTunes App Store or Android Market. The server handles access, versioning and updating of the applications.

When a new version is available the user gets prompted to download and install it directly; for critical updates access to the application can even be blocked until it is updated.

Secure Enrollment

Enrollment uses a challenge-response procedure, where the user enters an activation code provided through other authenticated access or by the SAF server administrator.

Native Corporate App

With SAF it is easy to make a corporate app that is safe to use in every device. The SAF framework can also include Mobilis DynApp*, which makes creating native apps as simple as webapps. SAF provides employees with corporate secured applications that can access intranet information or shared folders on their desktop PC.

Secure Data Storage

SAF includes the option for secure offline data storage. All data is encrypted on the device and users can view and edit content offline. It is convenient to be able to access data when the device is offline, e.g. travelling by plane or train. The encryption is based on public and private key and implemented with the best encryption offered by the platform. Data is encrypted and signed at all times.

Secure communication

All communication uses both client and server certificates with 2048 or 3072 bit keys. All data is signed by the transmitter and encrypted for the receiver. Third party certificate authority (CA) can be used or the server can act as CA.

* See DynApp white-paper

Secure Caching

For most resources, it is appropriate to allow that they be cached for some period of time. This reduces latency in accessing the document and lowers network traffic while keeping the data up-to-date. Caching of data for a resource is in accordance with the policy defined for that resource.

Access Revocation

Access to application resources or all applications can be remotely revoked for a single user or group of users. The next time the user tries to access this resource, the request will be denied. It is also possible to revoke an application when it is required that it ceases to be used. This also applies to the data stored by the application.

Resource Policy

Policies can be applied for data, functionality and time periods. All resources can be categorized into policy classes where the application is controlled to manage the resource in certain ways:

- no local storage/browse only
- no caching
- expiry date
- access time periods
- read only
- additional authentication

This provides a fine grained resource management both at group and user level.

Secure Data API

The essence of SAF is to provide simple access to data without exposing any of the complexity of how the data is accessed. Applications which use SAF can more easily be classified as secure by security officers since all handling of data and access to the backend must go through the framework. Security officers can feel at ease because the policy and access parameters in the service are configured according to the corporate security policy.

Background Update

Resources that are allowed to be stored locally can be configured to be updated without user interaction. This background update is secured and can allow data to be served through a “push” model rather than a “pull” model. Users always have access to the latest data and can be notified when updates are available. SAF also includes functionality to send messages to the users.

Administration

All administration tasks are accomplished via an easy-to-use, self-explanatory web interface allowing administrators to accomplish the full range of systems administration tasks. This keeps training time to an absolute minimum and provides for quick deployment. It includes functionality for management of applications, users, policies and revocation.

Implementation

SAF is well-packaged and can be installed on a standard application server supporting Java EE. This server is normally deployed at the customer premises and is managed by the customer. WIP can also provide managed instances of the server to organizations that prefer not to manage their own infrastructure.

The installation also includes documentation for management and development of the system.

The development documentation includes API, tutorials and example applications. Included are also ready-made components for the most common services such as email, file and intranet access.

Summary

Securing data by app management rather than by device lockdown gives both the company and the user greater security and freedom to effectively achieve their objectives.

With SAF by WIP you can embrace the new trends of BYO without having to worry about your information ending up in the wrong hands due to lack of sufficient infrastructure whilst facilitating maintenance and support of mobile devices.