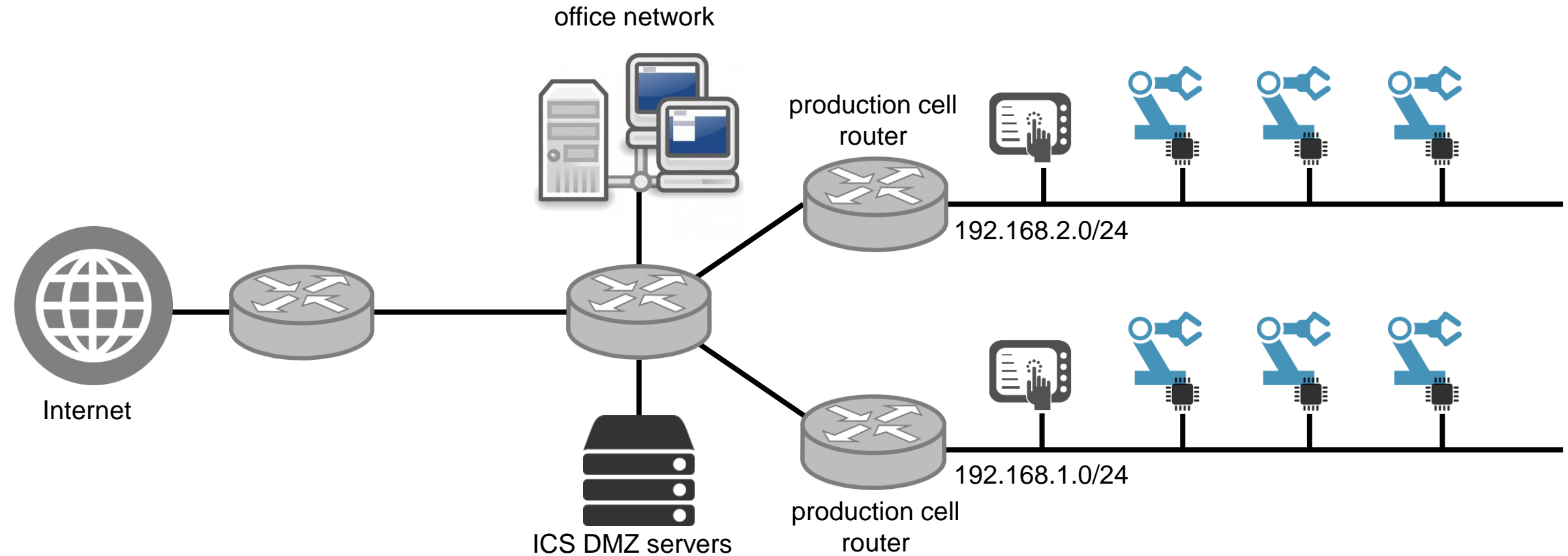


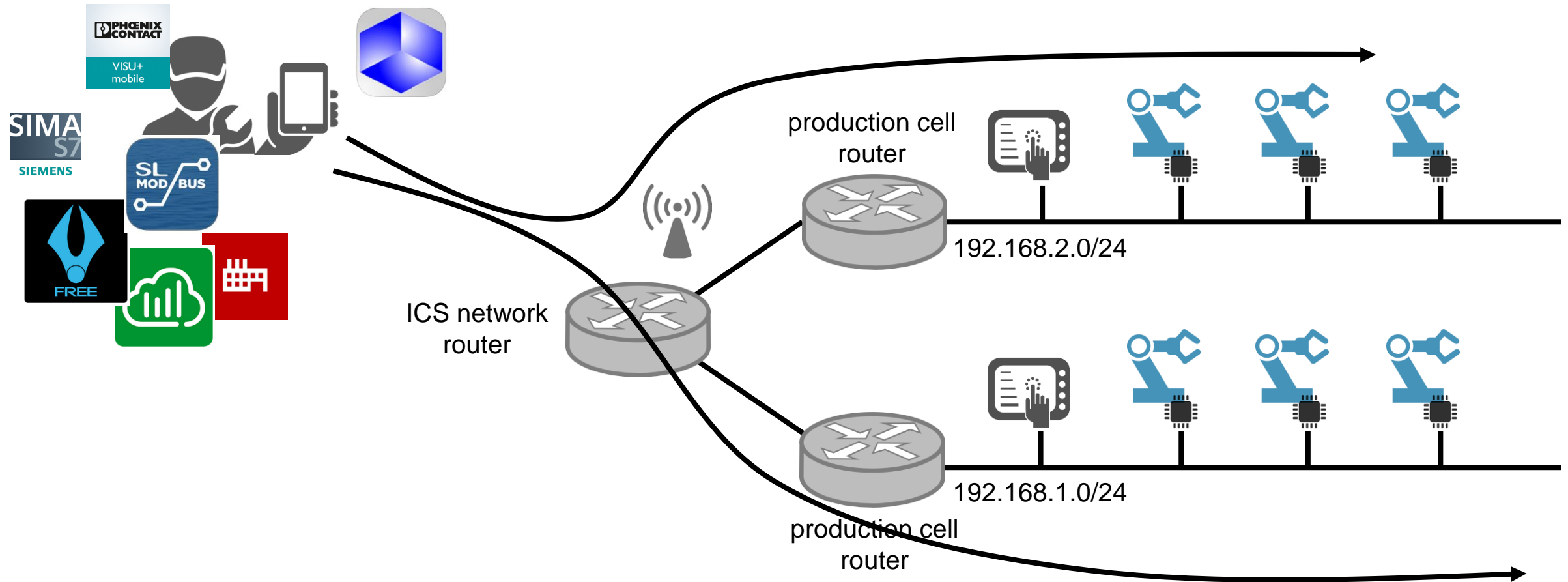
Secure Mobile Access to the Local ICS Network

Jan Vossaert
Veilige industriële netwerken
29/09/2016

Introduction



Introduction



Introduction

- Industrial Mobile Apps: Who's Using Them and Why
 - <http://www.automationworld.com/mobility/industrial-mobile-apps-whos-using-them-and-why>

*“We use the app to **monitor** our gas detection devices, but we also use a few controls in the app that allow us to **remotely silence the alarms...**” (Bayer Corp. in Pittsburgh)*

*“We have a few in-house mobile applications for **handling work orders and purchase orders**, as well as preventative maintenance and inventory.”*

*“A mobile HMI **reduces communication errors** between people by allowing the **field operator** to access the same data as the **control room operator**.”*

*“...**monitor** any area of production—packaging status, cook temperature or frying capacity—from the palm of their hands...”*
(Hillshire Brands)

*“...anytime **access to real-time and historical production data** and trends, operators can see where there are problems, where problems might potentially arise, or where additional capacity exists to increase production or run an alternative product.”*
(Hillshire Brands)

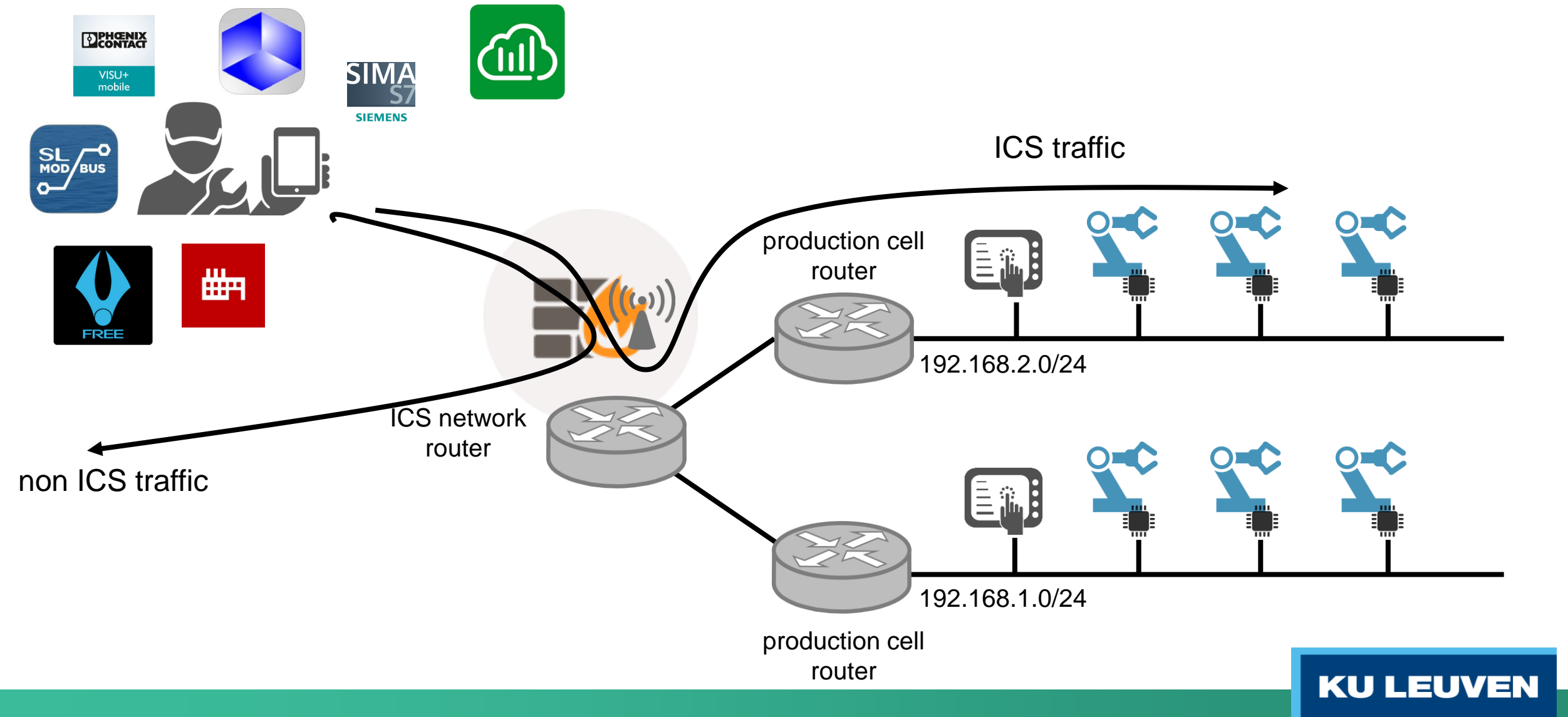
Introduction

- Use mobile devices in ICS environments
 - Hardware platform
 - Cheap off-the-shelf hardware
 - They're compact, lightweight, affordable, and readily available.
 - They offer powerful processors and rich UI capabilities
 - Rich wireless communication interfaces
 - Application platform
 - ICS equipment vendors have started to provide mobile app support
 - Applications that interact with corporate or other services
 - Built-in security technologies (VPN/MDM/app sandboxing/...)

Requirements

- Functional requirements
 - Use mobile to interact with ICS equipment
 - Use mobile to access company resources/services in back-end
 - Access resources on the internet
- Security requirements
 - Only traffic from specified ICS apps can reach the ICS network
 - Only authorized employees can access ICS network (via WiFi)

Solution Architectures



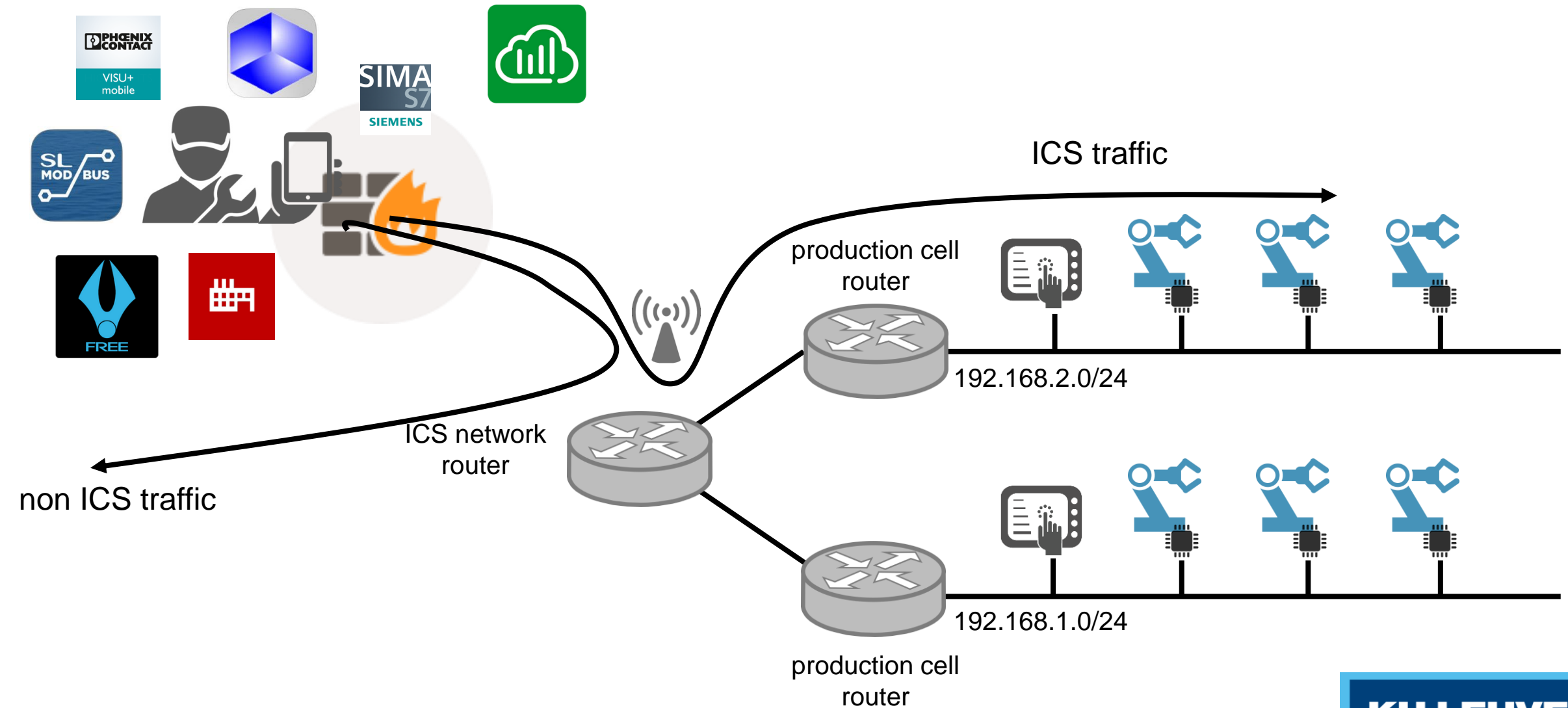
Solution Architectures

- Firewall-based solution
 - ✓ Separates most traffic nicely
 - ✓ Can match with expected network signatures
 - ✗ Malicious apps targeting ICS equipment
 - ✗ Other apps generating traffic for ICS network



Lack of required context information

Solution Architectures

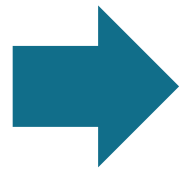


Solution Architectures

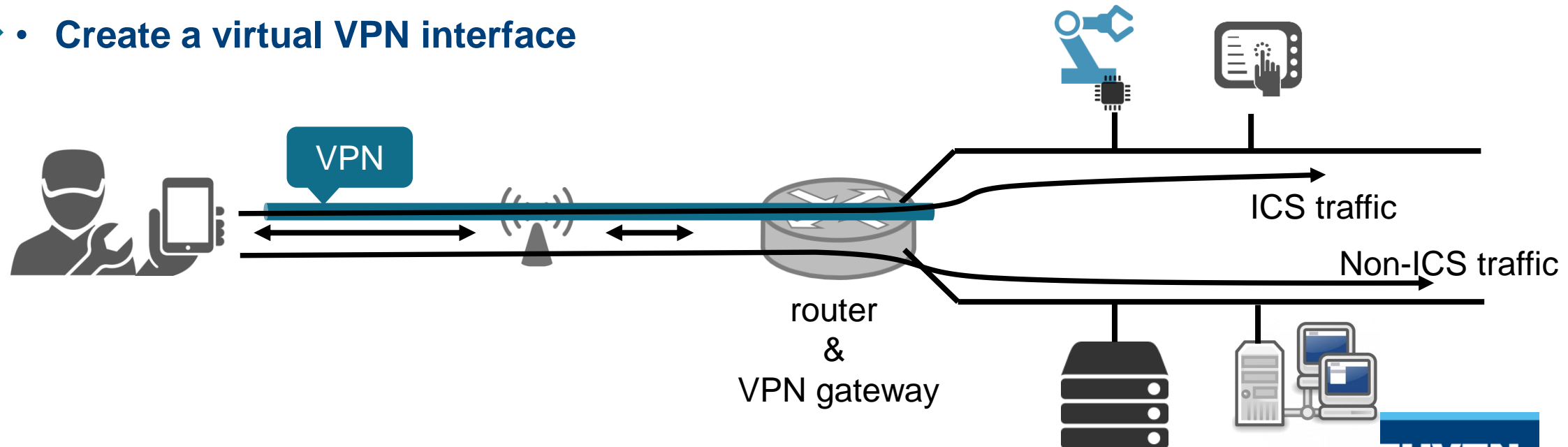
- MDM-based solution
 - COSU: Corporate-owned, single-use
 - “kiosks” or “purpose-built devices”: one application is intended to run on the device
 - Simple but greatly restricts use of mobile device
 - Provided by Android via **lock task** mode
 - Requires application awareness
 - Activated via MDM or enforced by application
- COBO: Corporate-owned, business only
- COPE: Corporate-owned, personally enabled
- BYOD: Bring your own device

Solution Architectures

- MDM-based solution
 - Create application/context-awareness by managing traffic on the mobile device
 - Usually all traffic passes through the same interface
 - Can we separate ICS and other traffic?



- **Create a virtual VPN interface**

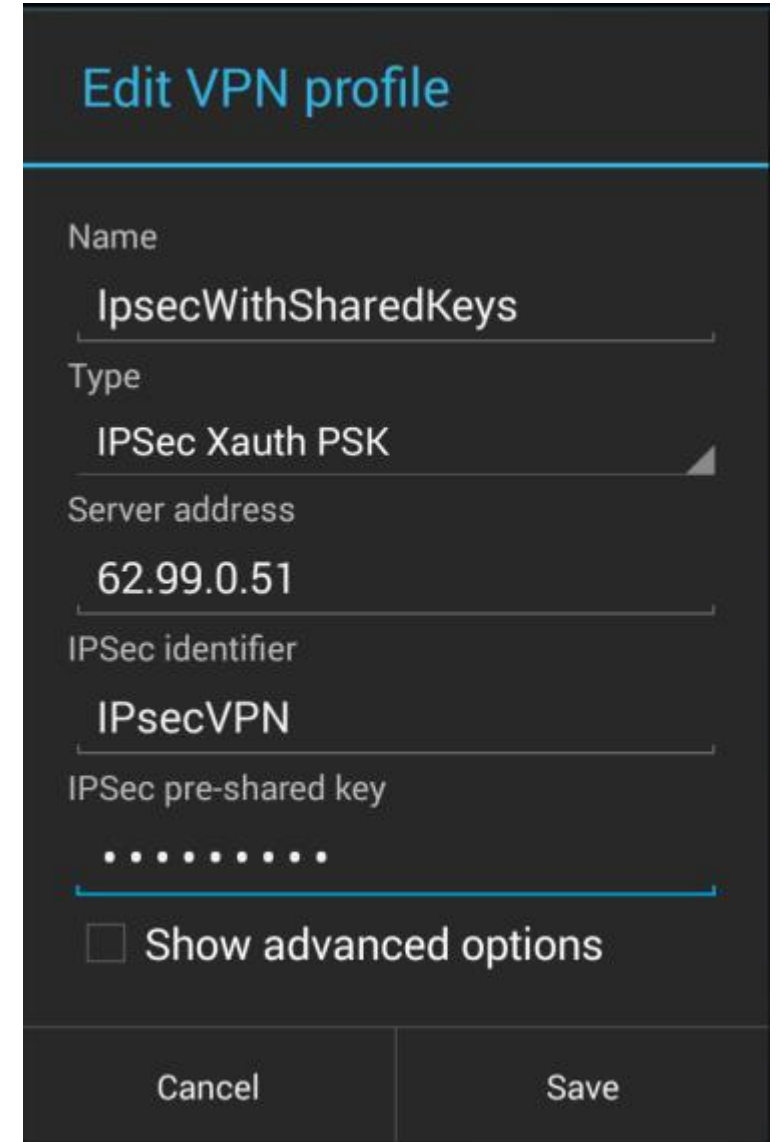


Background

- VPN technology on Android
- MDM on Android (Android for Work)

VPN Technology on Android

- Android has a built-in IPsec VPN implementation
 - Both PSK and RSA device authentication
 - Password-based user authentication
 - Does not support fine-grained control
 - White listed apps, MDM-based configuration



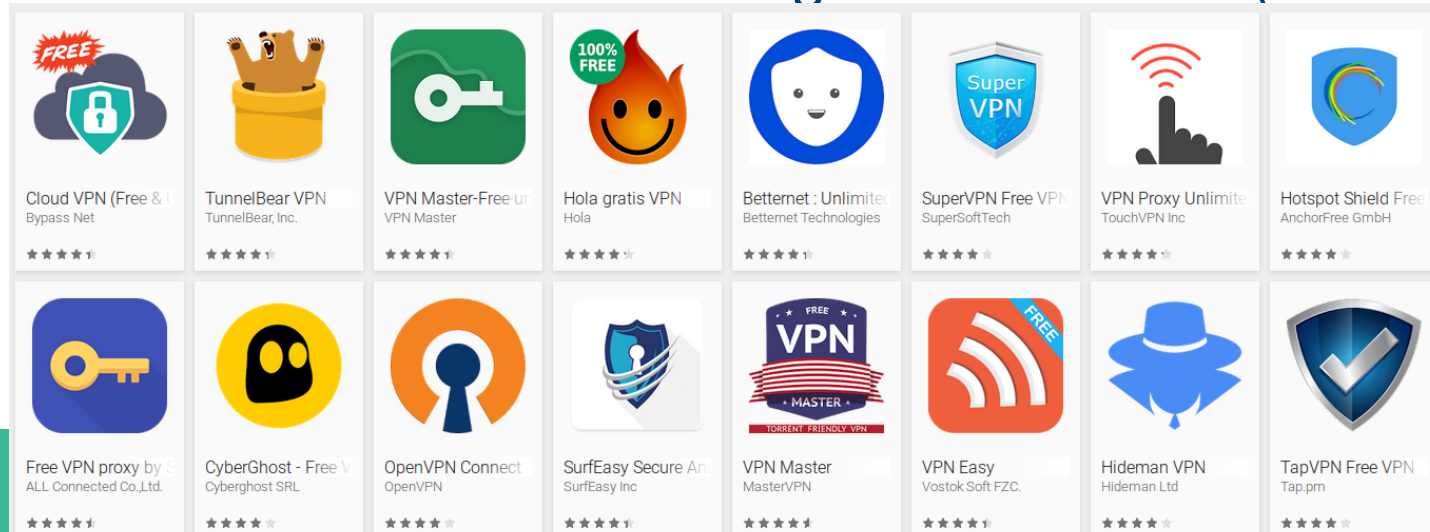
The screenshot shows the 'Edit VPN profile' screen in Android settings. The title is 'Edit VPN profile'. Below the title, there are several fields for configuring the VPN profile:

- Name:** IpsecWithSharedKeys
- Type:** IPsec Xauth PSK
- Server address:** 62.99.0.51
- IPsec identifier:** IPsecVPN
- IPsec pre-shared key:** A field with 10 dots, indicating a masked password.
- Show advanced options:** A checkbox that is currently unchecked.

At the bottom of the screen, there are two buttons: 'Cancel' and 'Save'.

VPN Technology on Android

- Android has a built-in IPsec VPN implementation
 - Both PSK and RSA device authentication
 - Password-based user authentication
- The Android framework provides APIs to develop VPN applications
 - Mainly OpenVPN ports
 - Interface also used for firewalling internet traffic (no root required)



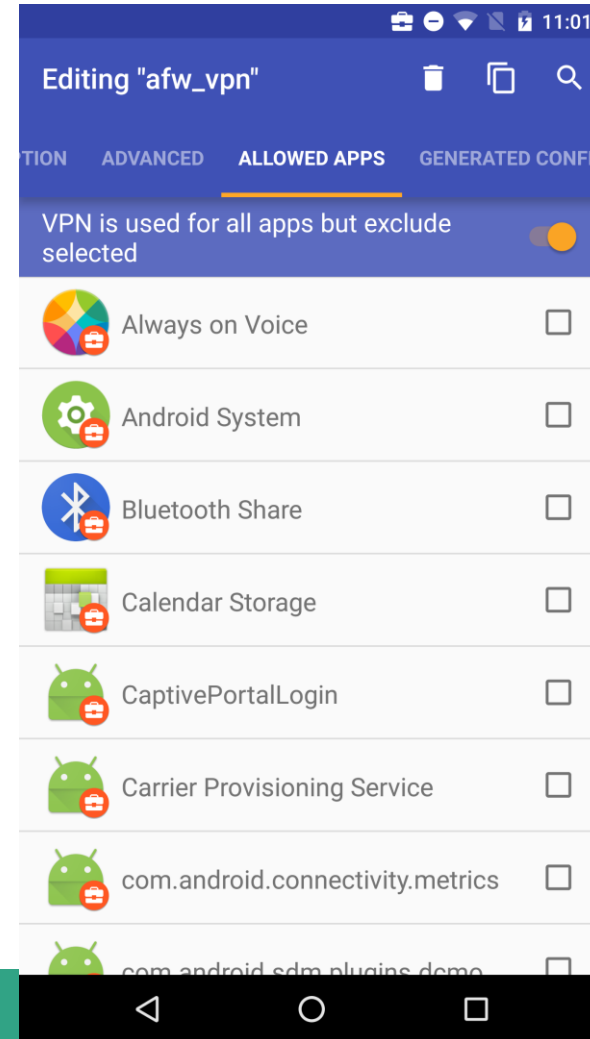
VPN Technology on Android

- Android has a built-in IPSec VPN implementation
 - Both PSK and RSA device authentication
 - Password-based user authentication
- The Android framework provides APIs to develop VPN applications
 - Mainly OpenVPN ports
 - Interface also used for firewalling internet traffic (no root required)
 - Some clients connect with predefined VPN servers
 - Some pure VPN client implementations

VPN Technology on Android

- Android provides APIs to allow VPN implementations to allow/disallow specific applications access to the VPN

<code>VpnService.Builder</code>	<code>addAllowedApplication(String packageName)</code> Adds an application that's allowed to access the VPN connection.
<code>VpnService.Builder</code>	<code>addDisallowedApplication(String packageName)</code> Adds an application that's denied access to the VPN connection.



Android for Work

- Platform from Google that improves Android usability, security, and flexibility in work environments
- Built-into recent Android devices (5 and higher)
 - Newer Android versions add more features
- Supports two virtual profiles on Android device
 - Person profile managed by user
 - Work profile managed by employer

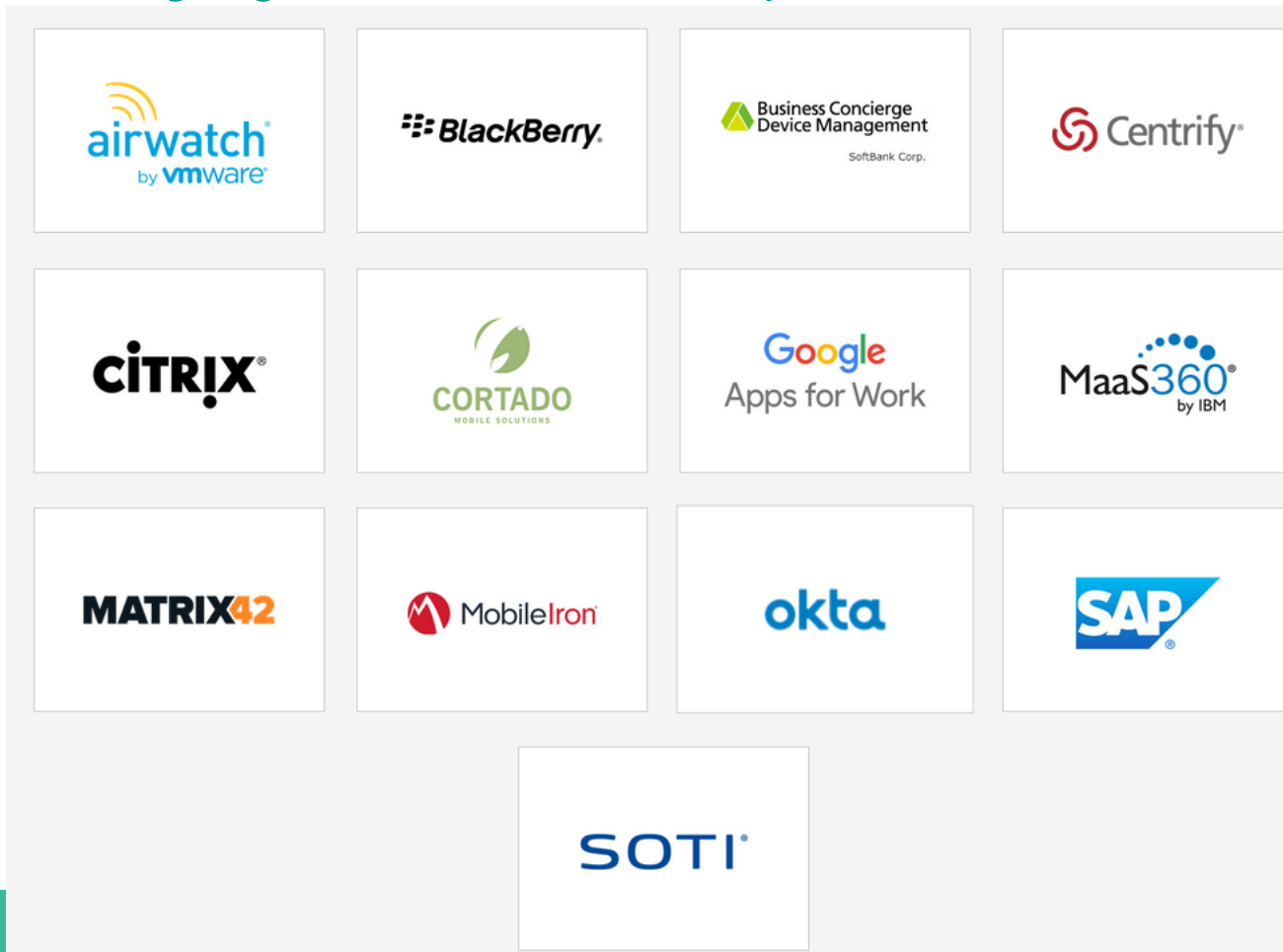
Android for Work

- AfW APIs are used by Enterprise Mobility Management (EMM) providers to enforce company policies

System-wide policies/settings	Work profile policies
Controlled sharing of data between profiles	Specify apps that can/should be installed in the work profile
Password policies	Auto wipe profile upon synchronization failure
Require full disk encryption	Credentials for access to company networks/services
Allow camera	App-specific policies/configurations for work apps
Allow developer options	Share content from work to personal profile
Allow screenshots	Copy/paste content from work to personal profile
Allow configuration of network access	...
Allow reset to factory settings	

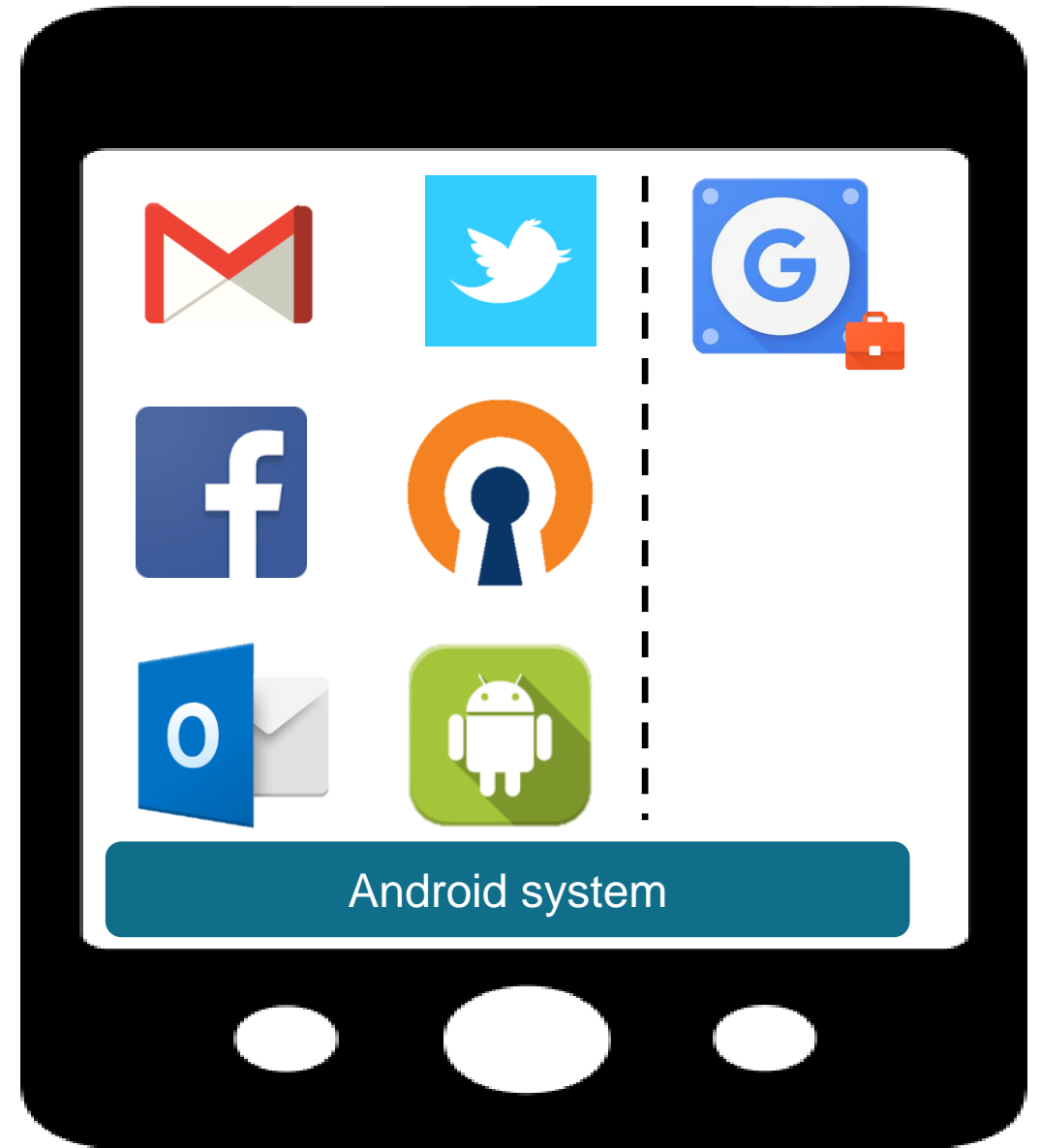
Android for Work

- APIs/capabilities are used by Enterprise Mobility Management (EMM) providers
- <https://www.google.com/work/android/partners/>



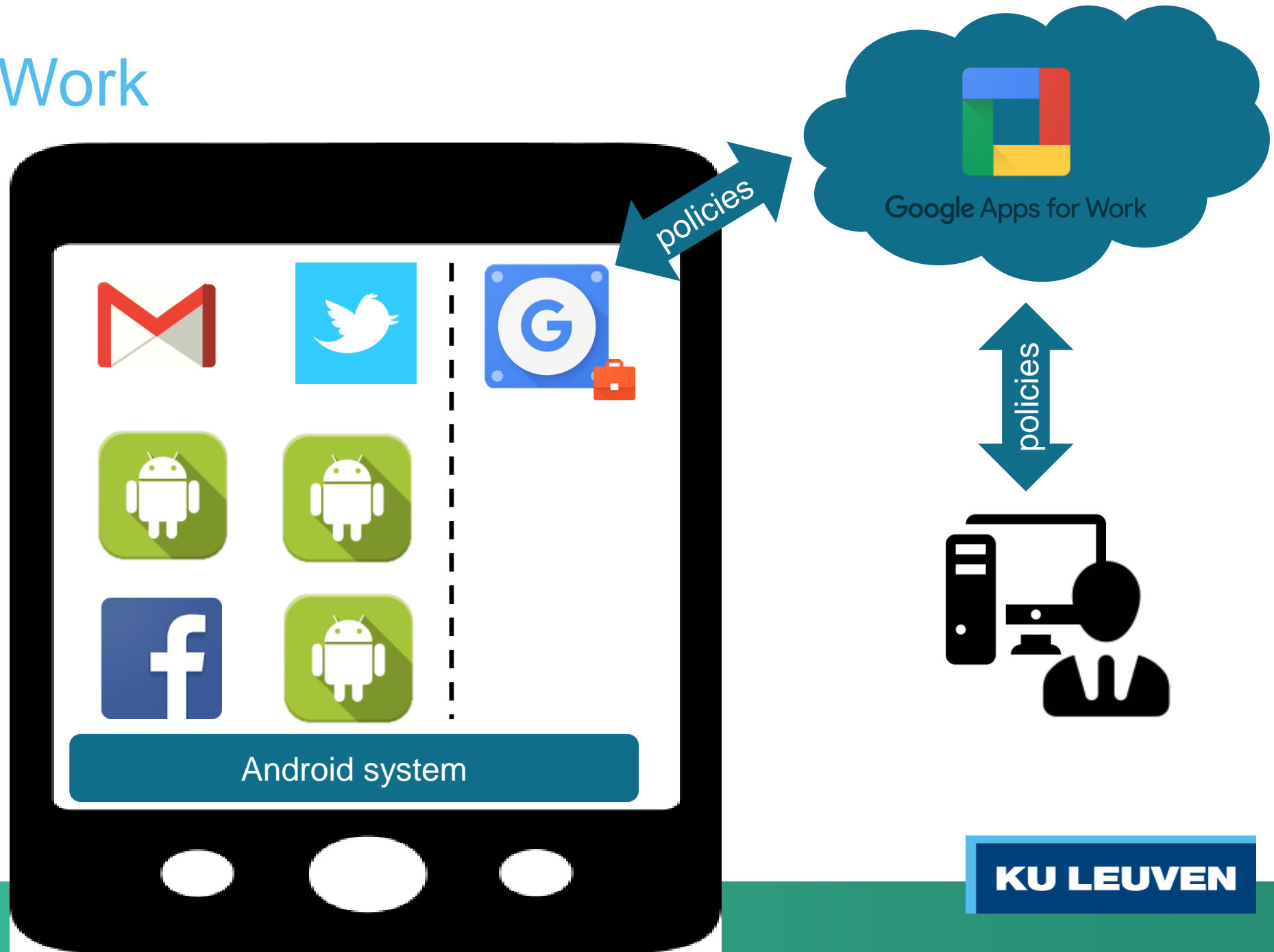
Android for Work

- Device enrollment
 - Install EMM app on device
 - EMM app creates work profile
 - Policy-based isolation between both profiles
 - Control over company profile via MDM



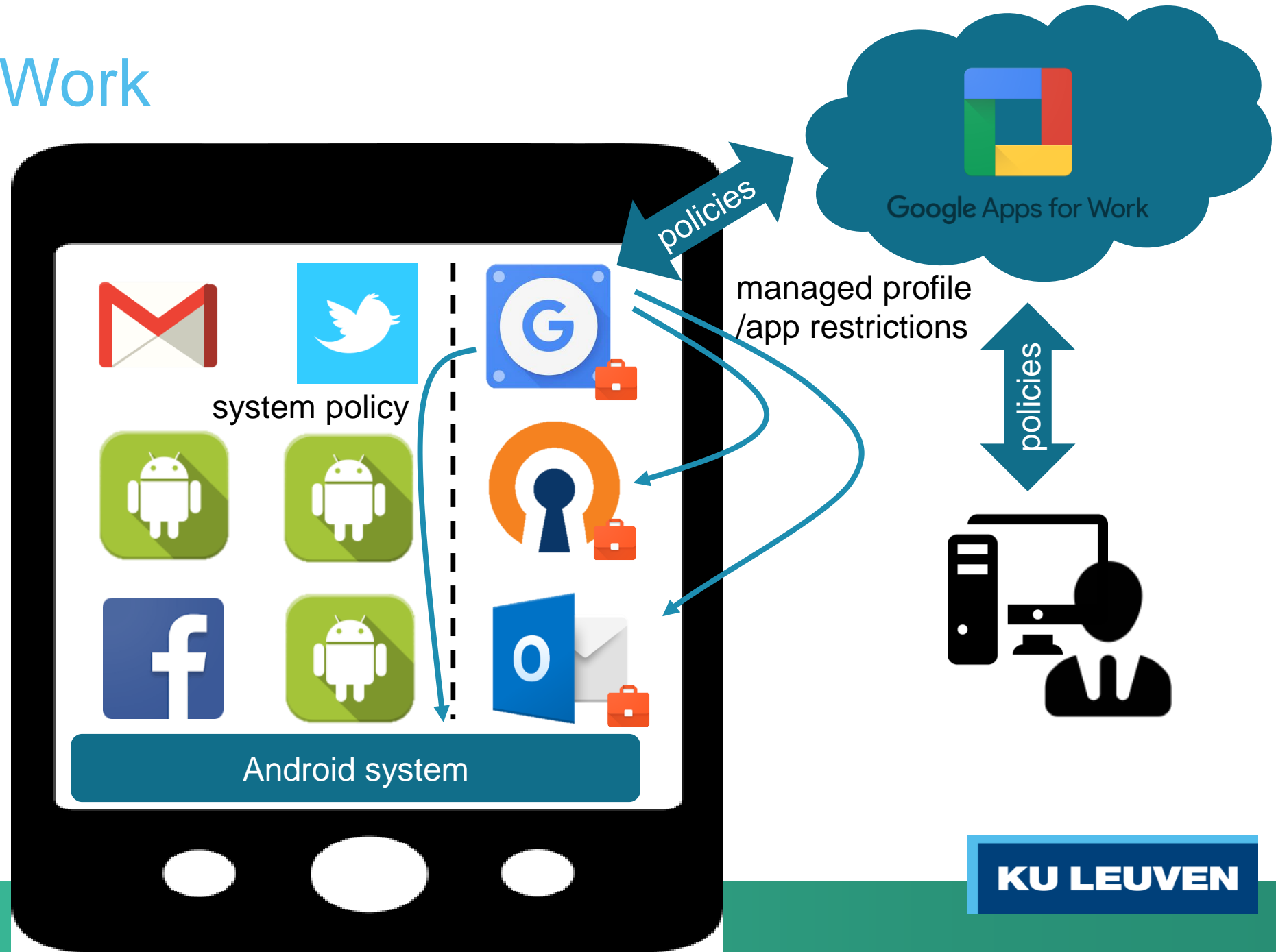
Android for Work

- Policy specification



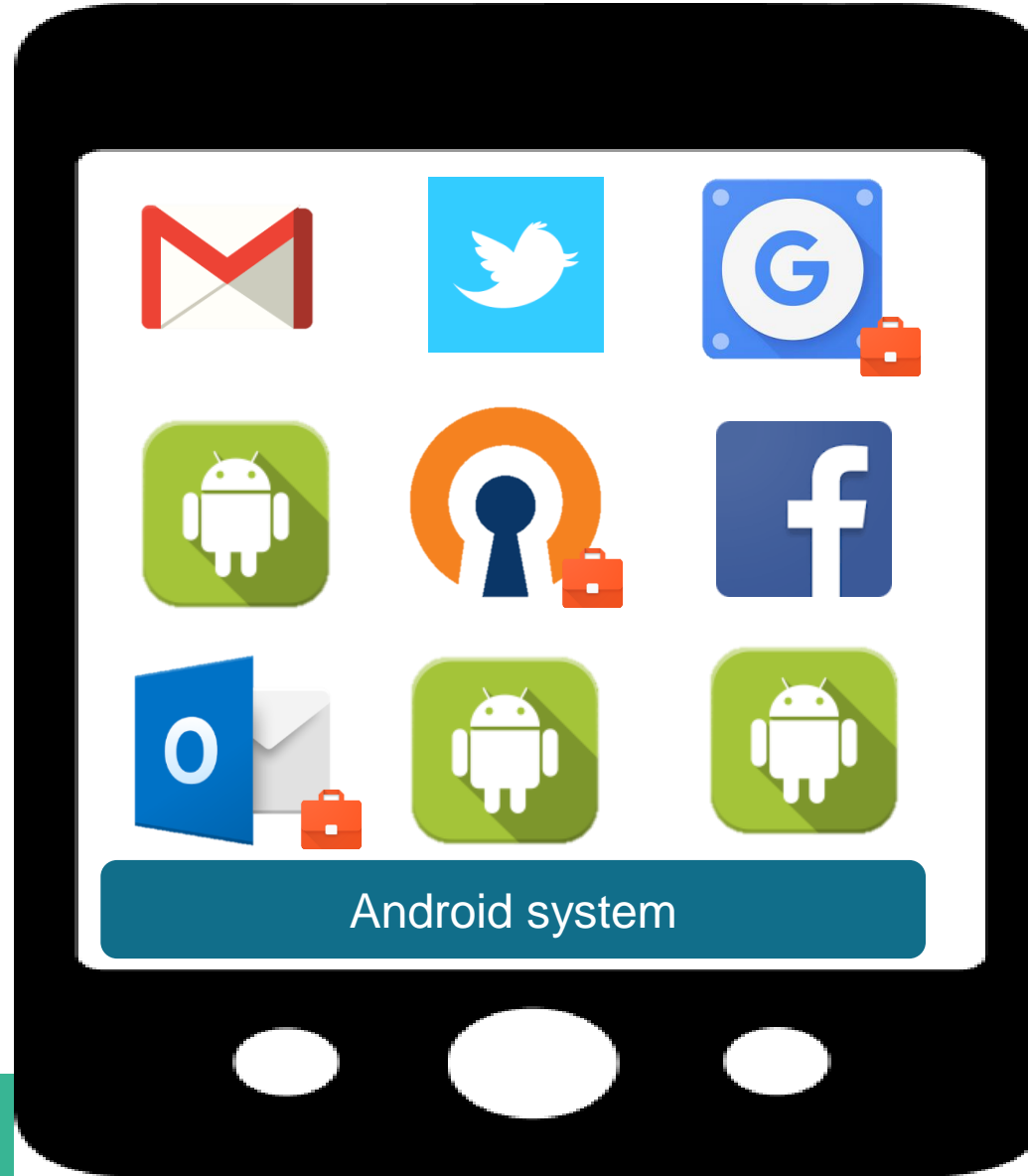
Android for Work


- Policy enforcement



Android for Work

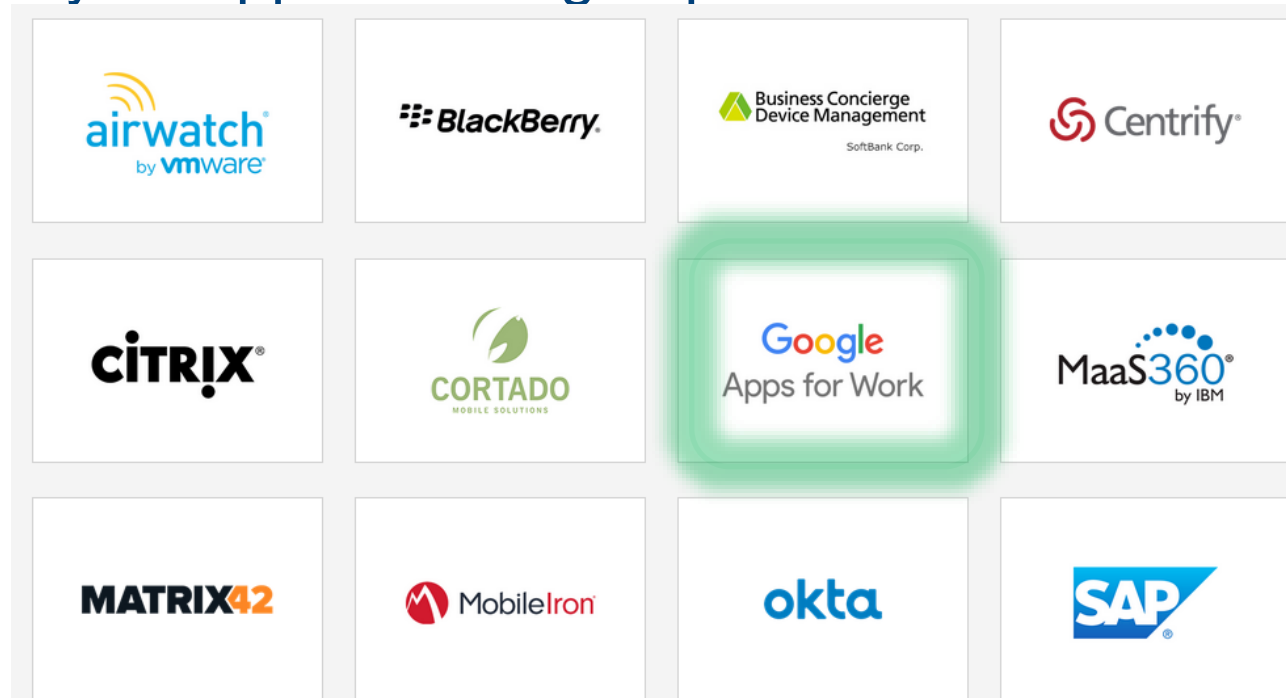
- Policy enforcement



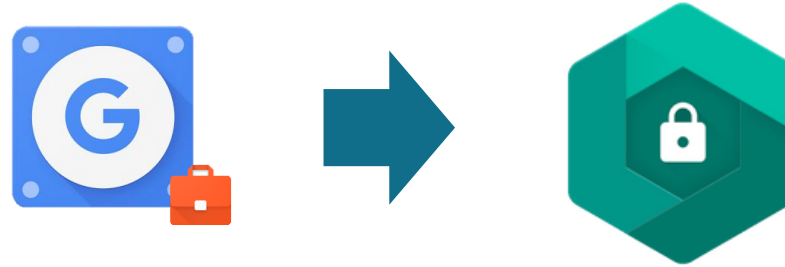
- User has both work and personal apps installed
- Users can have the same app installed in both the work and personal profile
- Each version runs in its own sandbox
- Users can distinguish between apps via 

Realization

- MDM providers
 - Preliminary tests with Google Apps for Work
 - Does not yet support managed profile



Realization



Test DPC

Sample developer Bibliotheek en demo

★★★★★ 28

PEGI 3

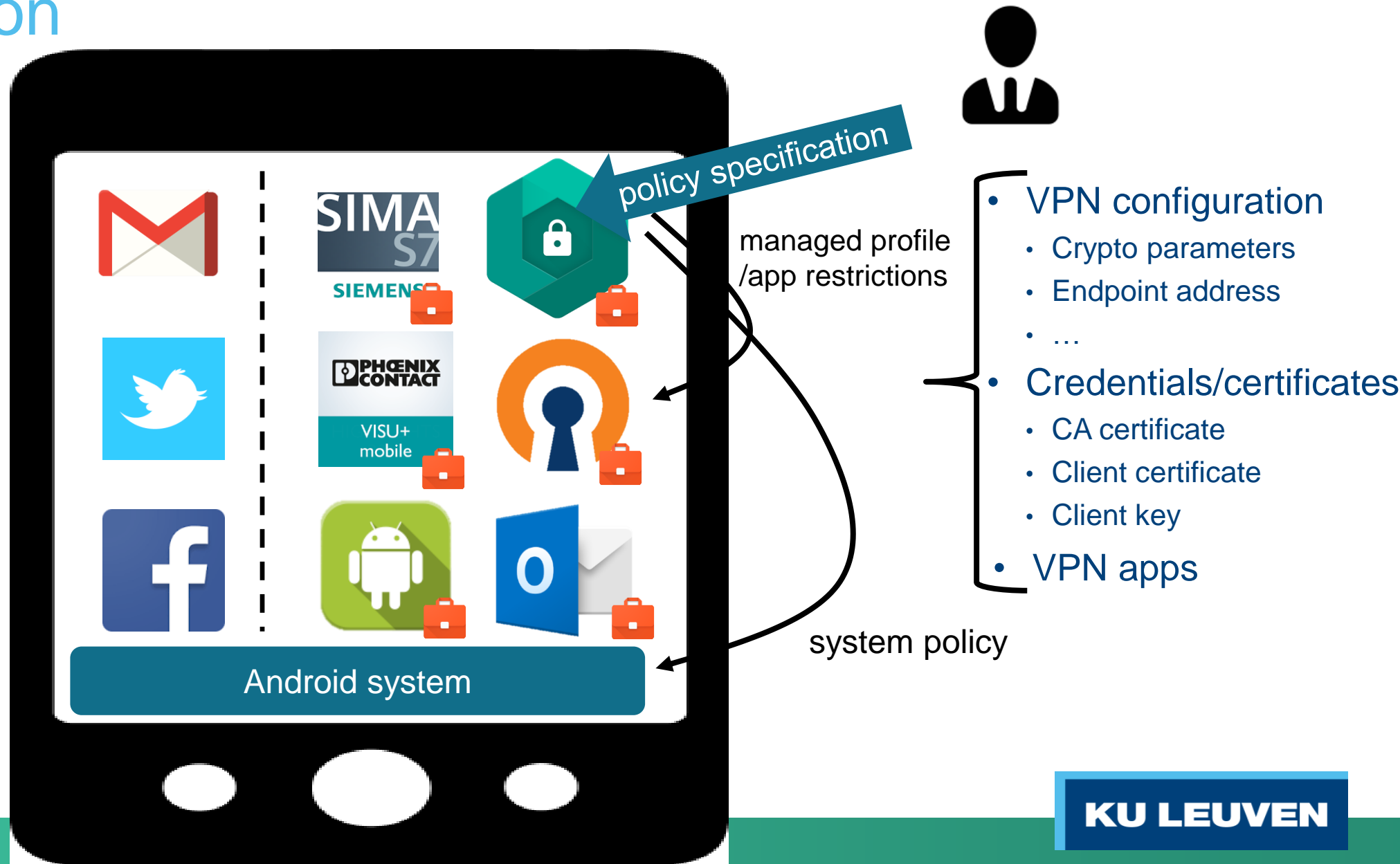
Deze app is compatibel met al je apparaten.

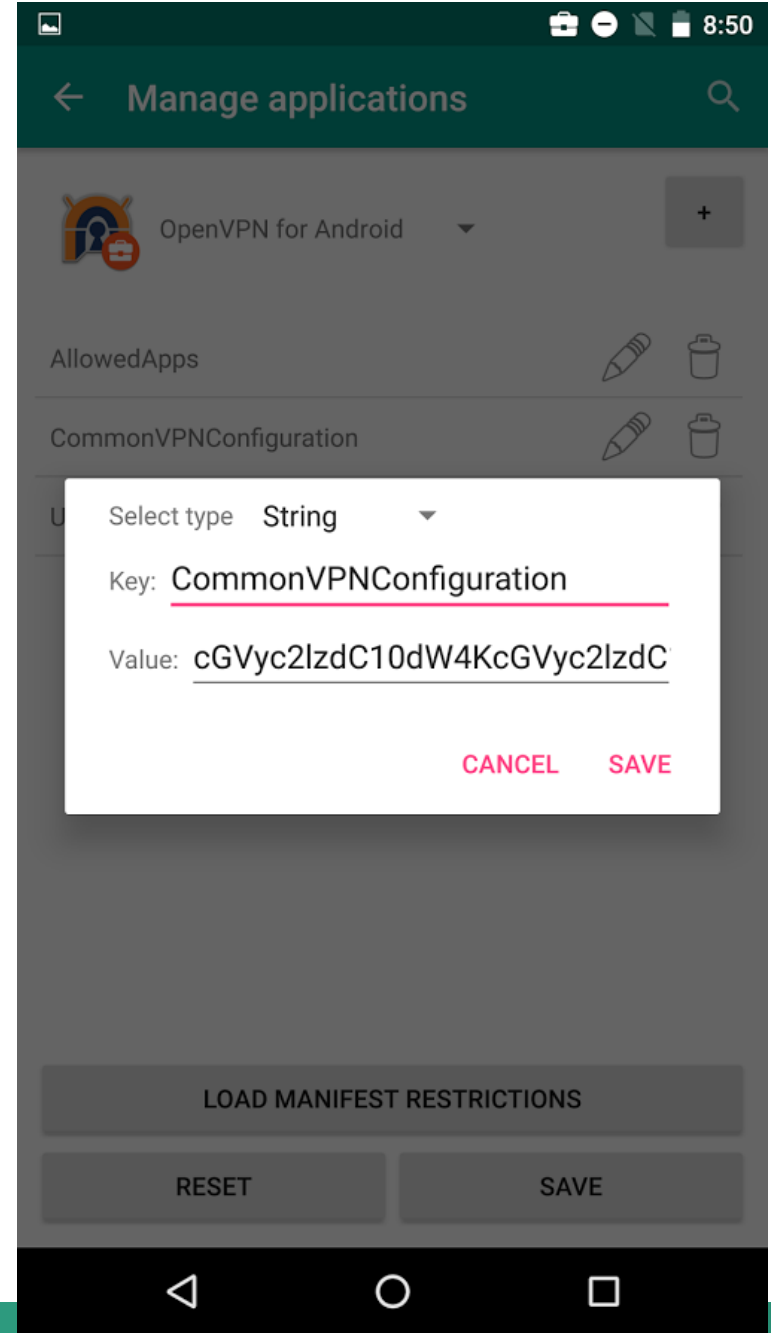
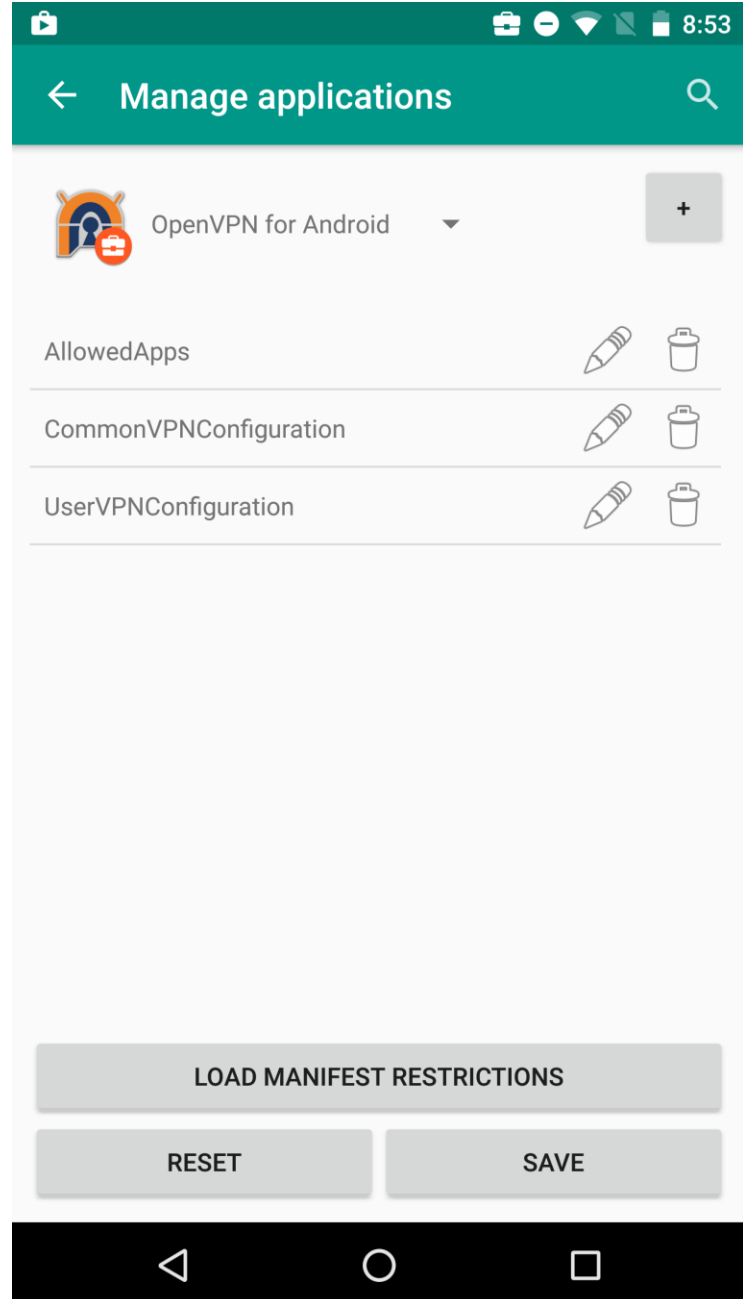
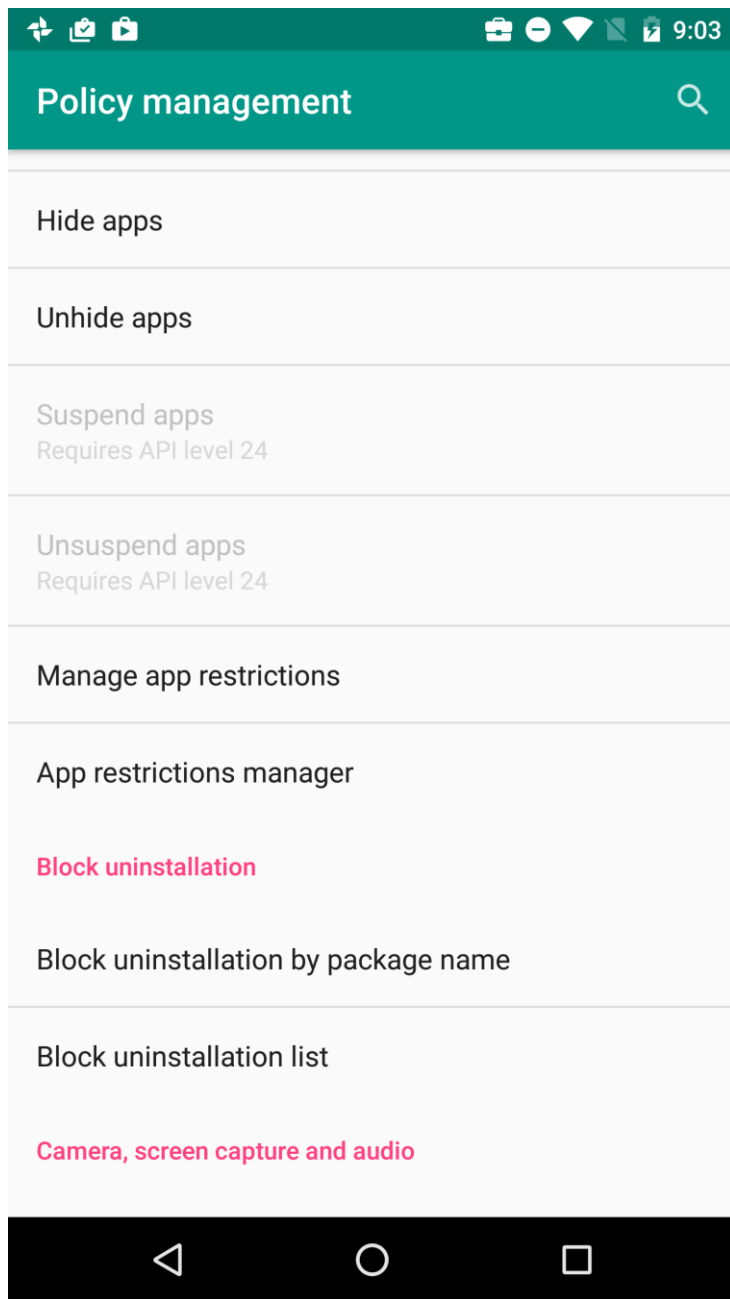
Toevoegen aan verlanglijstje

Installeren

- MDM providers
 - Preliminary tests with Google Apps for Work
 - Does not yet support managed profile
- Used Test DPC as an alternative
 - <https://play.google.com/store/apps/details?id=com.afwsamples.testdpc&hl=nl>
 - Sample device policy controller for use with Android for Work
 - Client-side specification of policies
 - Set up work profile
 - Enable work apps
 - Set applications restrictions
 - Manage security policies
 - ...

Realization



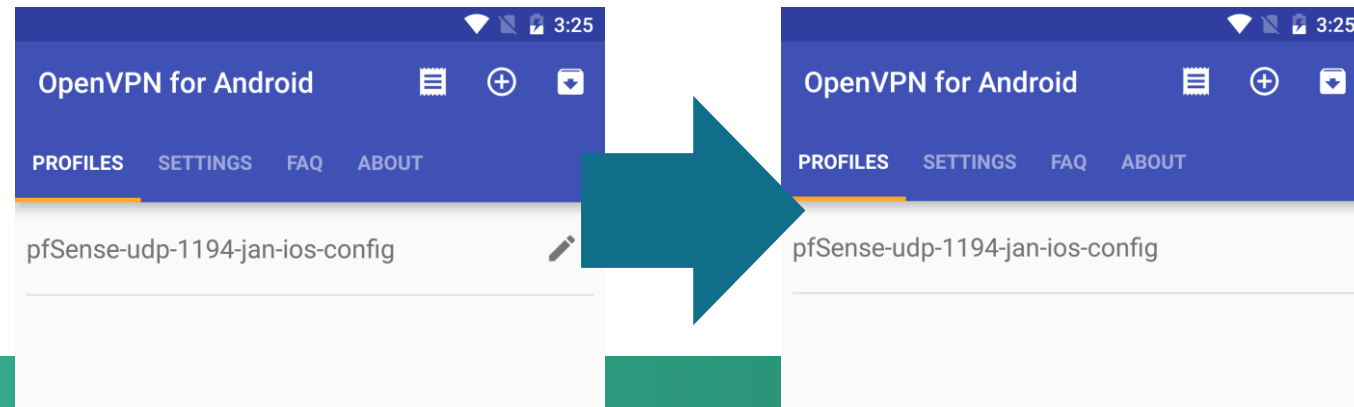


Realization

- Unfortunately most apps do not yet implement managed profile API
 - A popular OpenVPN client is open source (Apache 2 license)...
 - <https://github.com/schwabe/ics-openvpn>
 - <https://play.google.com/store/apps/details?id=de.blinkt.openvpn>

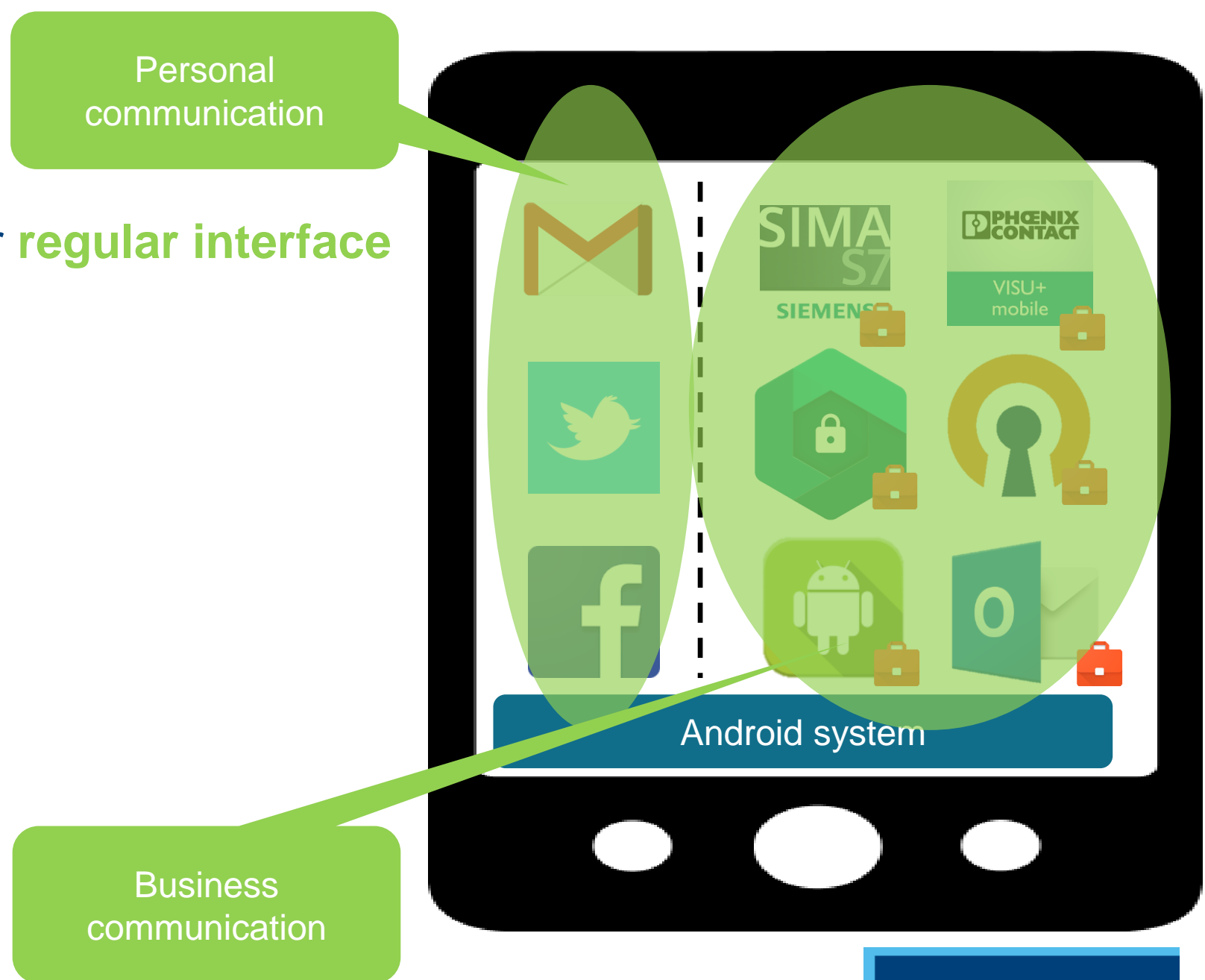


- Extended implementation
 - Added Managed Profile support
 - Disabled on-device configuration



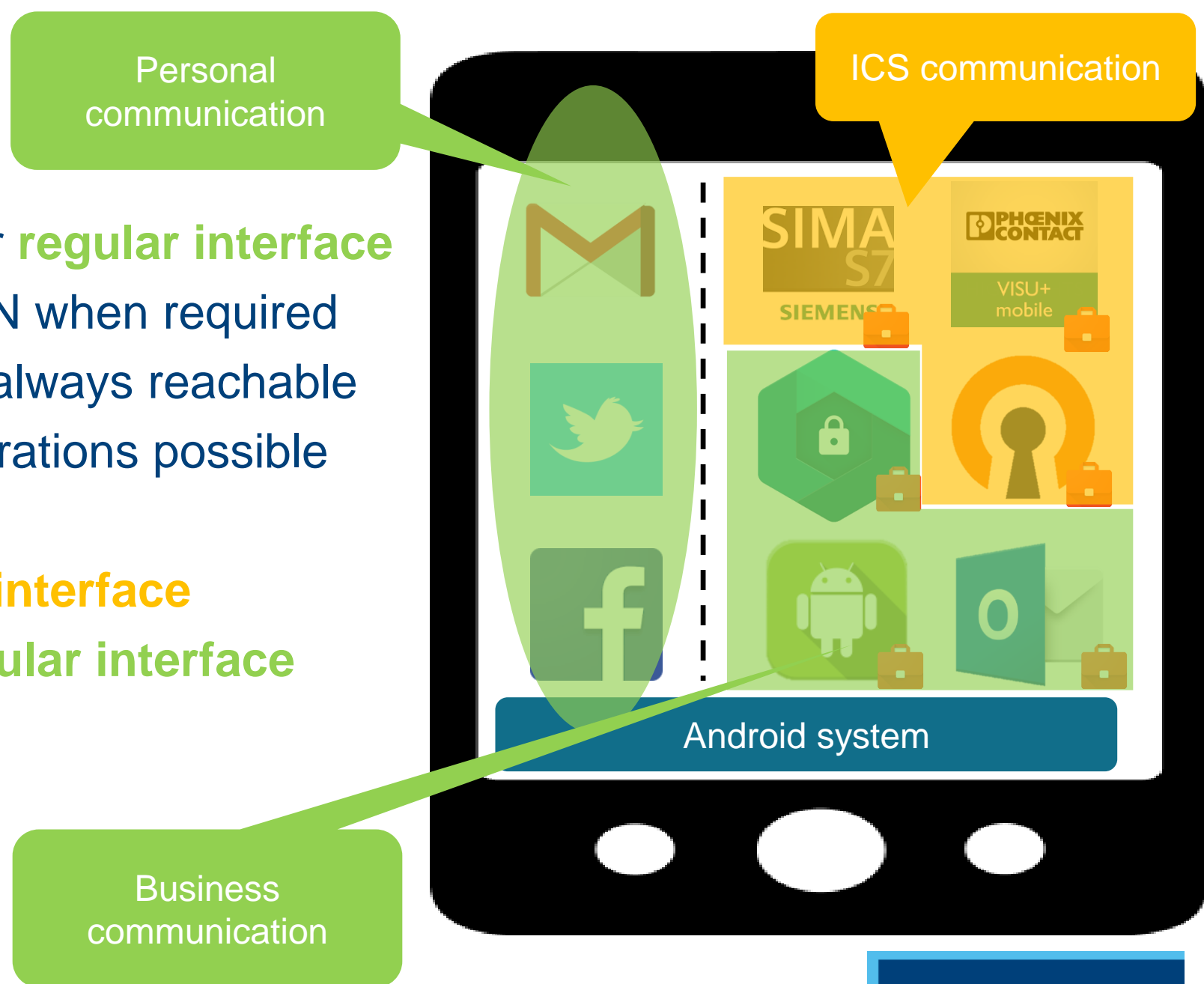
Realization

- By default all traffic over **regular interface**

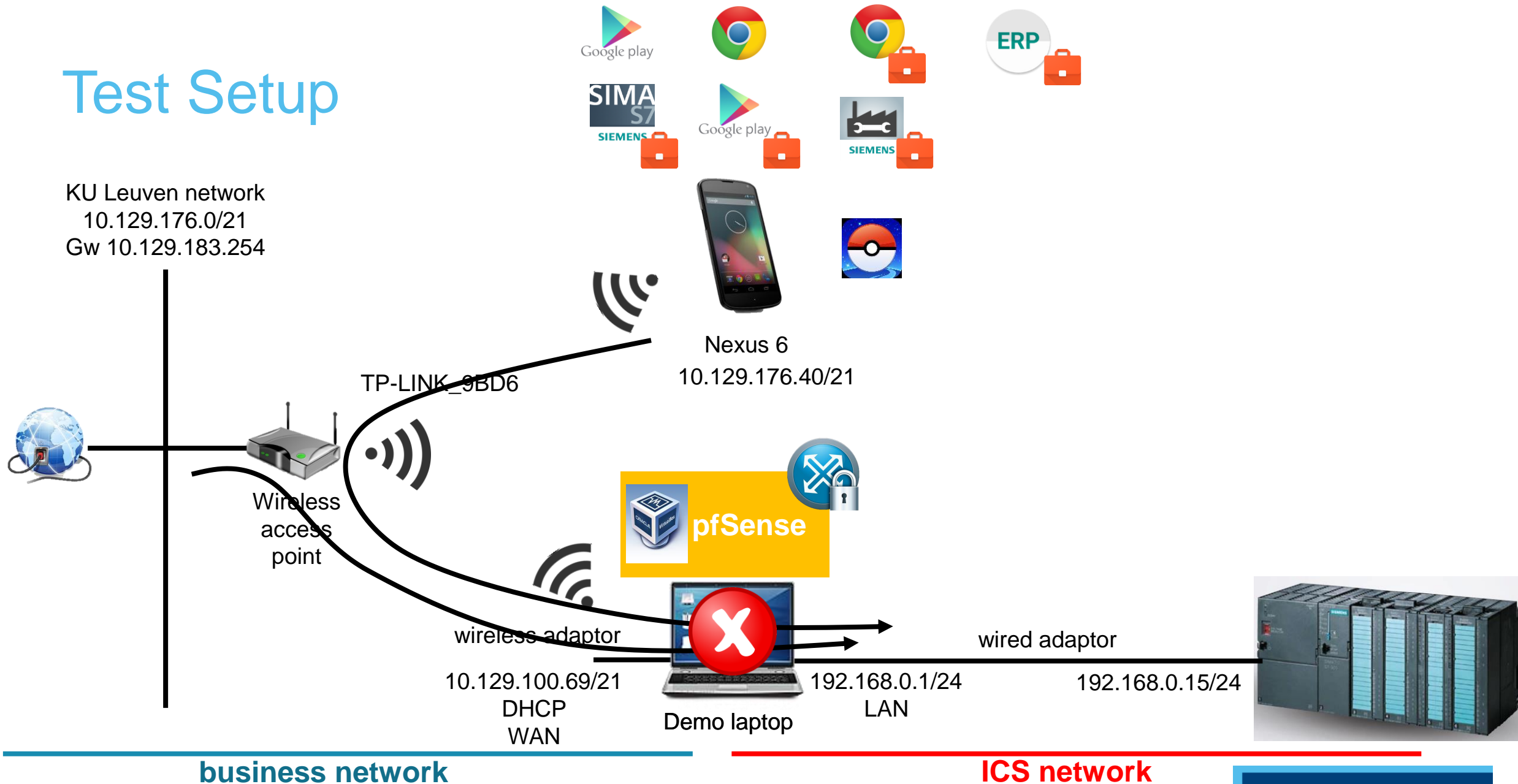


Realization

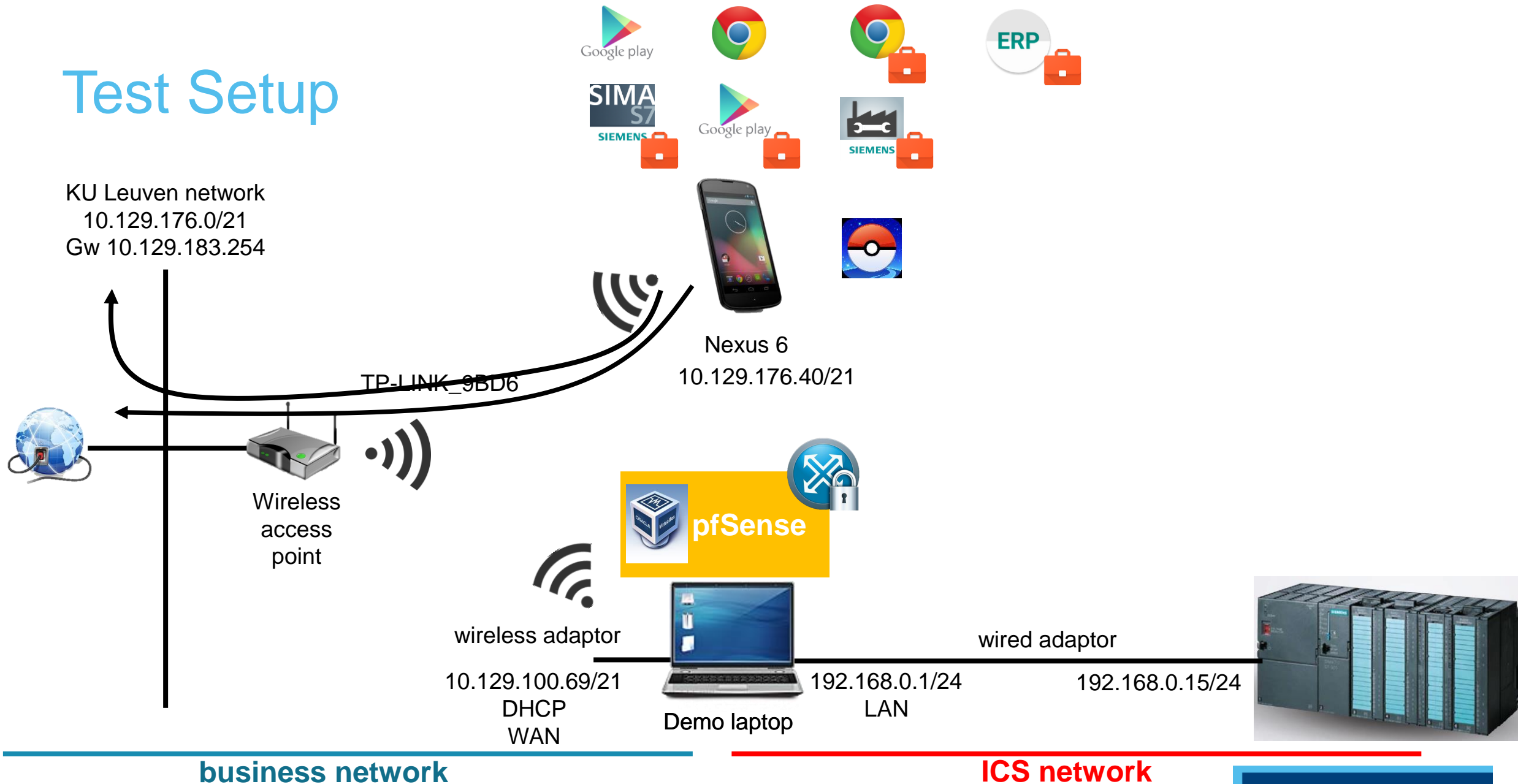
- By default all traffic over **regular interface**
- Employee activates VPN when required
 - VPN endpoint is not always reachable
 - Multiple VPN configurations possible
 - ICS traffic over **VPN interface**
 - Other traffic over **regular interface**



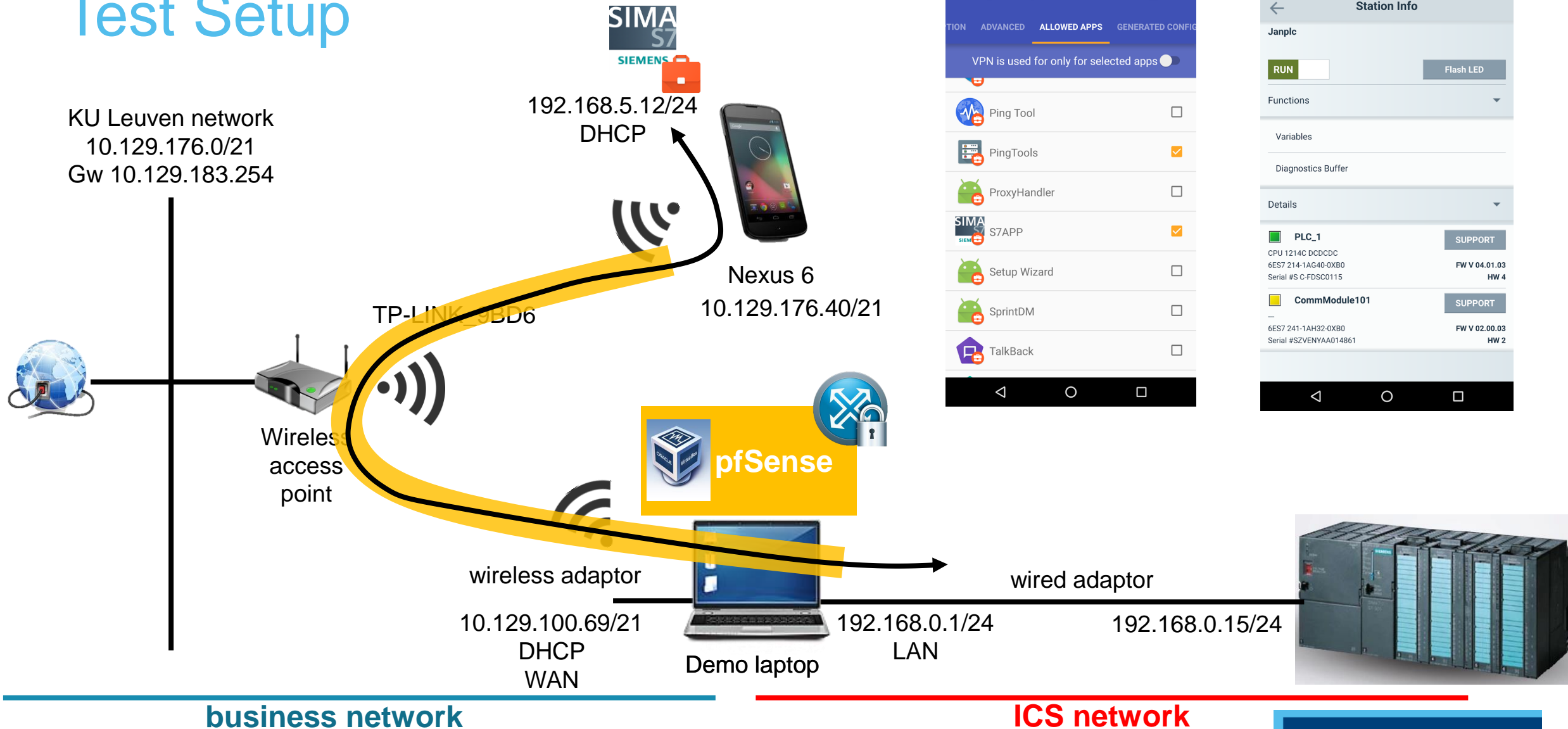
Test Setup



Test Setup



Test Setup



Evaluation

- Functional requirements
 - Use mobile to interact with ICS equipment ✓
 - Use mobile to access company resources/services in back-end ✓
 - Access resources on the internet ✓
- Security requirements
 - Only traffic from specified ICS apps can reach the ICS network
 - Only authorized employees can access ICS network (via WiFi)



- Malicious employees
- External attacker
- Malicious apps



- Malicious employees
- External attacker

Evaluation

- Malicious employees
 - Can access ICS equipment via app
 - Cannot copy configuration/credentials
 - User authentication and logging at VPN gateway (accountability)
 - Only specified apps can connect over VPN
 - Restrict functionality of app via Managed Profile
 - Requires application awareness



Evaluation

- External attacker
 - Access control to device
 - Secure passcode
 - Device encryption
 - Disable adb
 - Upon theft/loss
 - Remote wipe
 - Block credentials
 - ...



Evaluation



- Malicious apps
 - Isolation between work and personal profile (cannot access work profile VPN)
 - Work profile
 - Only traffic from specified apps in work profile is sent over VPN
 - MDM manages apps that can be installed in work profile
 - App sandboxing
 - Traffic analysis shows only allowed traffic in ICS network

Evaluation



- External attacker
 - Secure WiFi network (can be company wide)
 - Credential based access control of employees to ICS VPN gateway
- Malicious employee
 - Can access WiFi network
 - Has no direct access to credentials
 - Only allowed employees can access ICS network from managed app

Evaluation



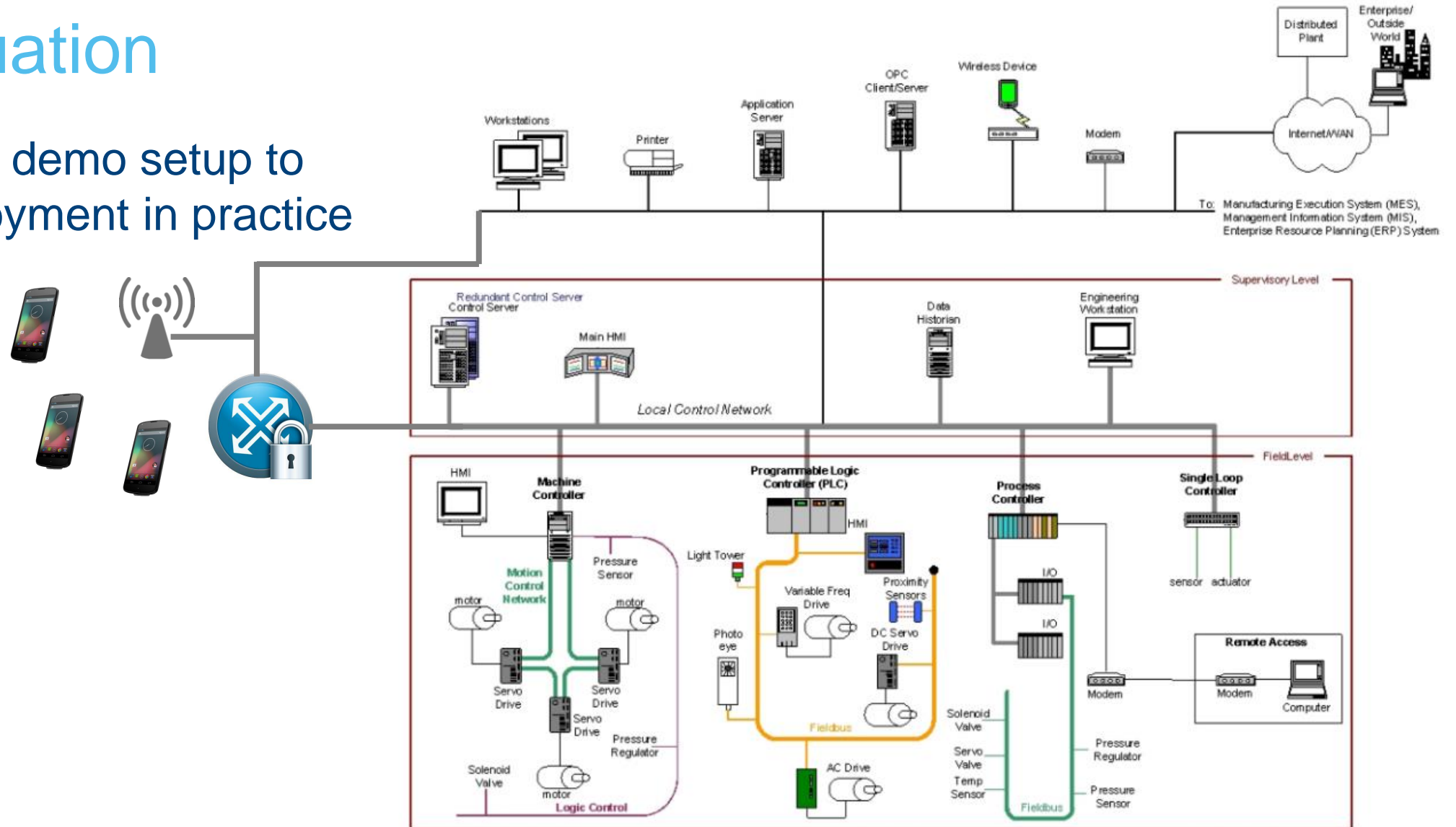
- Security depends on software integrity of trusted computing base



- Keep software updated!
- Reactive measures
 - Remote wipe
 - Block credentials
 - ...

Evaluation

- From demo setup to deployment in practice



Evaluation

- From demo setup to deployment in practice
 - Android 5(+) devices – approved devices
 - Mobile device management
 - Management model
 - MDM provider which supports the required features (mainly Managed Profile)
 - Most apps still need to implement Managed Profile API (only small modifications required)
 - Logging

BULLETPROOF SSL AND TLS

Understanding and Deploying SSL/TLS and
PKI to Secure Servers and Web Applications



Ivan Ristić



Evaluation

- From demo setup to deployment in practice
 - Set-up PKI infrastructure
 - Industry-grade VPN gateway
 - pfSense deployment
 - Compatibility with ICS VPN router
 - Secure WiFi (xEAP)
 - User management
 - Employees
 - External service engineers

BULLETPROOF SSL AND TLS

Understanding and Deploying SSL/TLS and
PKI to Secure Servers and Web Applications



Ivan Ristić



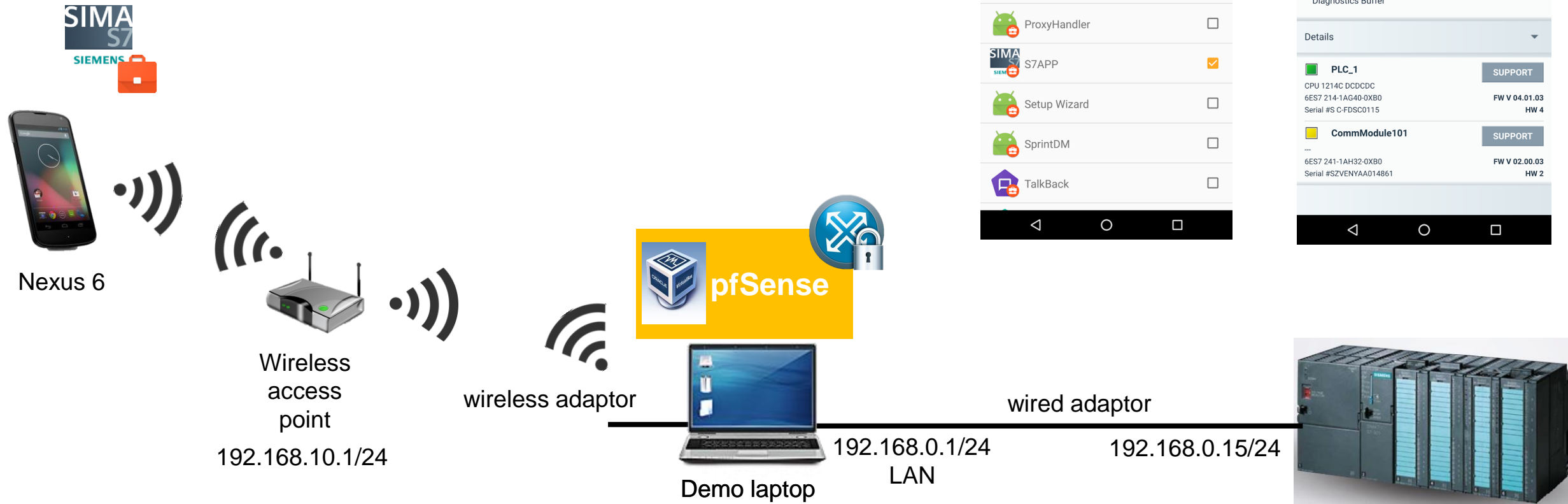
Evaluation

- From demo setup to deployment in practice
 - ✔ Simplified setup (without Managed Profile)
 - Only allow VPN and ICS-approved apps to be installed in work profile
 - Manual configuration of VPN app
 - ✖ Employees can access credentials to access VPN
 - Malicious
 - Careless
 - ✖ Limits flexibility in work profile

Conclusion

- Managed Profile provides interesting opportunities to tailor apps for specific corporate needs... but requires application awareness
- Google Apps for Work is not up to date with latest MDM capabilities of Android

Demo Setup



business network

ICS network

KU LEUVEN

