

SSL Reloaded (SSLR)

Visit Vestiacom – 17.09.2013

Tomasz Zielinski / Tom Kienle

TOPICS

Company Presentation Vestiacom

Staff working on SSLR

Demo – Milestone 1

SSLR Overview (Scope / Approach / Timeline / Milestones / Organization)

SSLR in depth (optional)

STAFF WORKING ON SSLR

						
Tomasz Zieliński	Tomasz Krówczyński	Paweł Majerczak	Mateusz Słupny	Inga Soprun	Patryk Mencfeld	Anna Sypiańska
Project Manager / Software Architect	Team Leader / Lead Java Developer	Senior Java Developer	Lead C Developer	Junior C Developer	iOS/Android Developer	QA
<ul style="list-style-type: none">. Tomasz has over 15 years of experience in system architecture and developing secure and mission critical systems.. Tomasz has broad experience in architecting and delivering large and complex systems.	<ul style="list-style-type: none">. Tomasz has joined Vestiacom in 2013, he has over 10 years of experience in developing Java applications (mostly backend).	<ul style="list-style-type: none">. Paweł has joined Vestiacom in 2010, he has over 5 years of experience in developing Java backend applications.. Paweł developed most of the HomeMonitor/ RemoteNAS backend code as well as many improvements in the SRS platform.	<ul style="list-style-type: none">. Mateusz has joined Vestiacom in 2010, he has over 4 years of experience in developing C/C++ applications.. Mateusz was responsible for developing most of the Device Client and HomeMonitor/ RemoteNAS Communication Library.	<ul style="list-style-type: none">. Inga has joined Vestiacom in 2013, she has 1 year of C/C++ software programing experience.	<ul style="list-style-type: none">. Patryk has joined Vestiacom in 2013, he has 4 years of overall software programming experience including 2 years programming iOS applications.	<ul style="list-style-type: none">. Anna has joined Vestiacom in 2010, she has 4 years of Java programming experience and over 1 year working as a QA.. Anna prepared and executed integration test plans for HomeMonitor.

ABOUT SSLR

SSLR is a new product category which empowers our customers to «keep an eye on what matters» – This is what matters to customers.

It's a combination of devices, mobile app and a cloud based service.

It consists of several interconnected devices like cameras, plugs & a unique multi-sensor-button. These can be combined and set up as desired.

It's part of a gateway ecosystem (not technically but marketing-wise).

Devices can be combined to scenes with unique properties, such as „Alarm System“ or even „baby-phone“. Users enjoy a great freedom when it comes to setting up the devices.

Users control their devices by a smartphone app and set up simple IFTTT style rules – e.g. «If camera detects movement recording is triggered and plug „Living room“ is set to OFF».

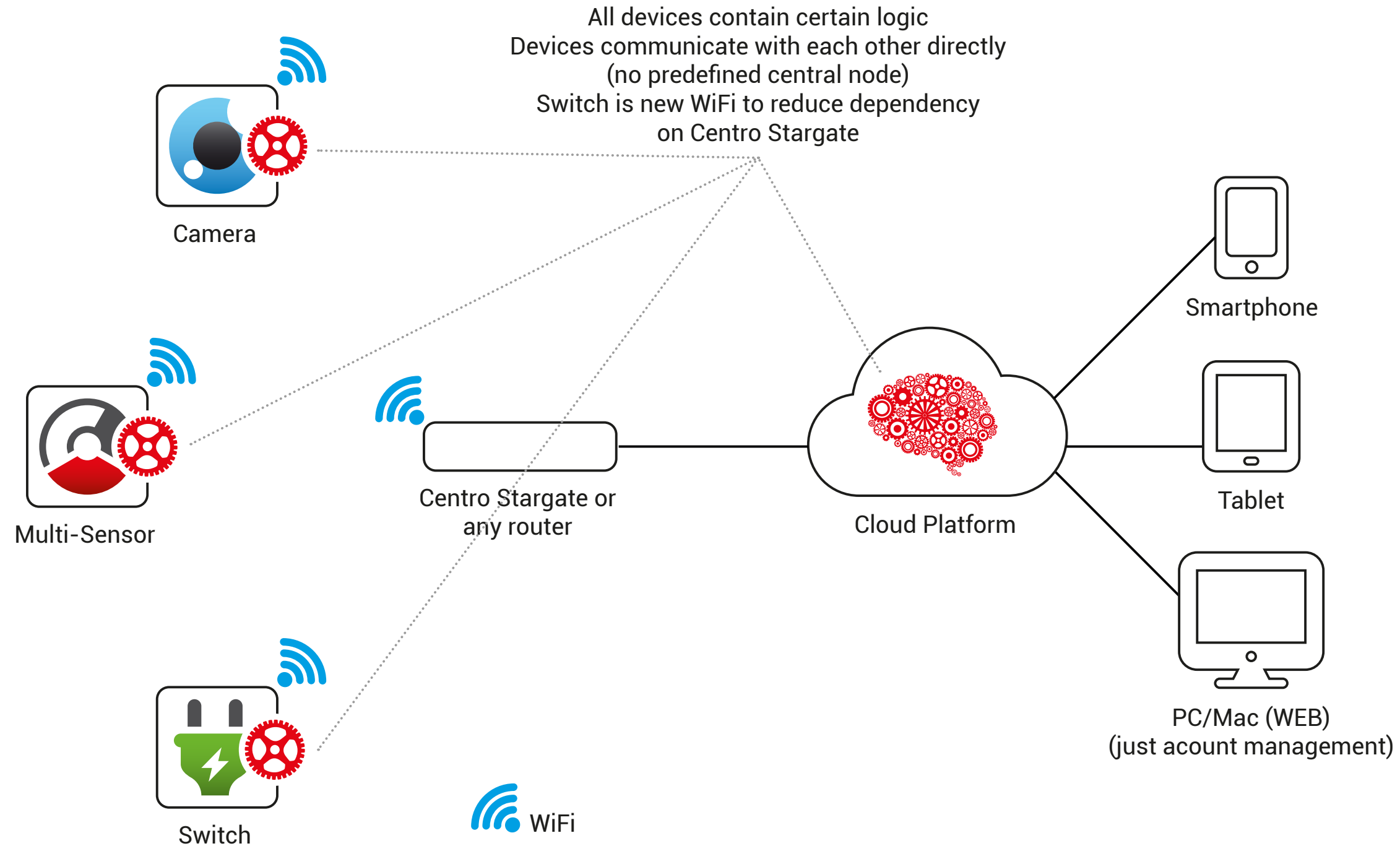
ABOUT US

Pragmatic
Agile
Track-Record
Entrepreneurs
Lean
Learning's
Motivated
Focussed
Trust

SIMPLICITY (AND GREAT CUSTOMER EXPERIENCE)

before buying	buying	installation	usage	get help
<ul style="list-style-type: none">. Clear value proposition. Communicate emotional apps (use-cases). Simple and affordable devices	<ul style="list-style-type: none">. Simple online-store	<ul style="list-style-type: none">. Simple registration process. WIFI integration with two buttons presses. Connected devices pop-up automatically in smartphone App. Configuring a device requires minimal input – just name and app	<ul style="list-style-type: none">. Hide everything which is not in focus. Focus on daily usage – make it obvious but surprise	<ul style="list-style-type: none">. Clever integration of help and tips. Help within 8 hours

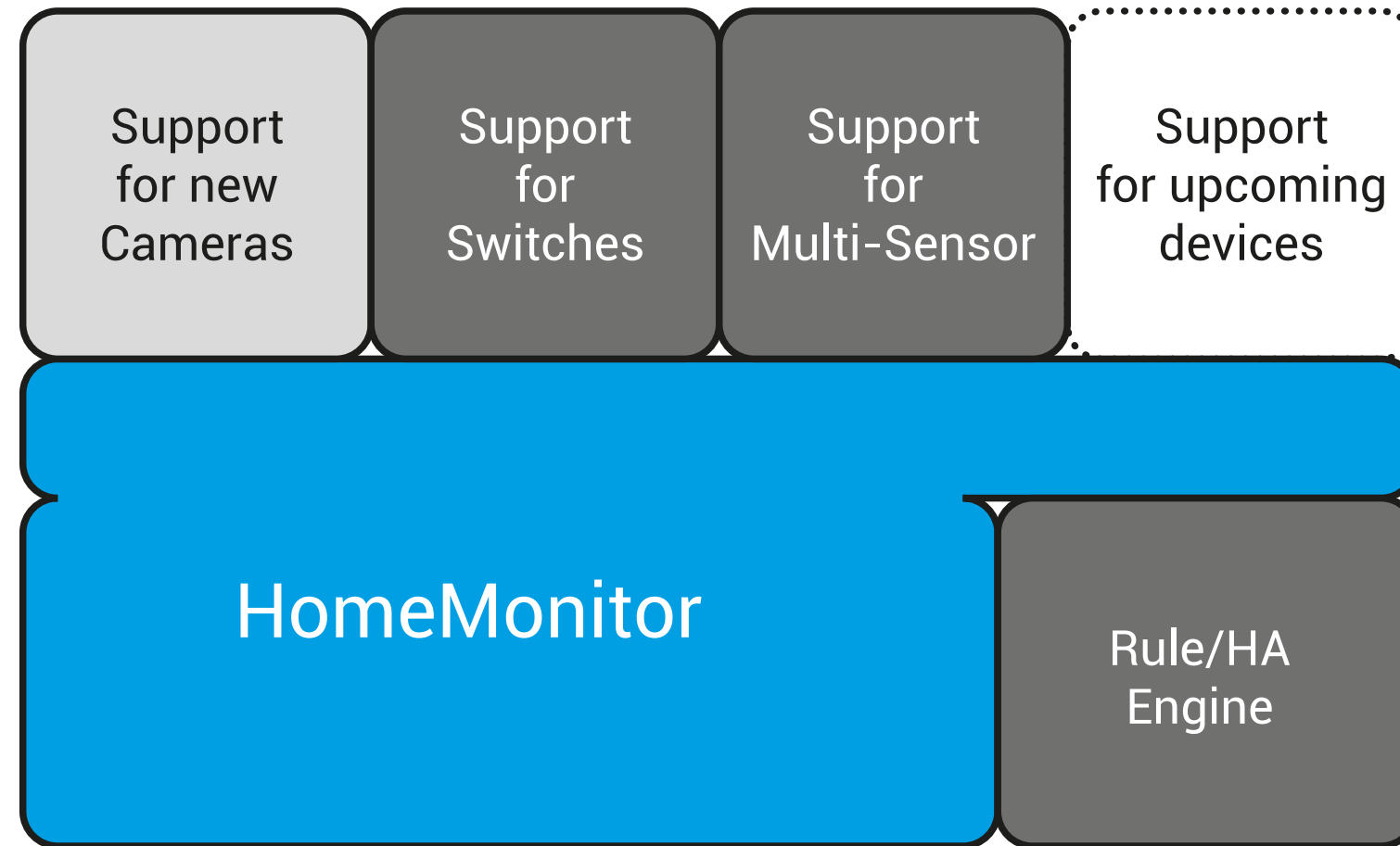
SCOPE / CONCEPT



CLOUD / HOMEMONITOR

HomeMonitor gives a head-start with ...

- IP Camera integration
- Reliable connectivity from anywhere
- Scalability
- Security
- DB
- REST APIs
- User/Account Management
- Sharing
- Admin GUI
- Logging
- more



 Existing & proven  Configuration & driver  New

DEVICES & APPS



← This is a device AND an app

DEVICES & APPS



This is the same device BUT
a different app

DEVICES & APPS



Devices can „run“ different apps (act different) – but only one@time.

APP – THE PARTS

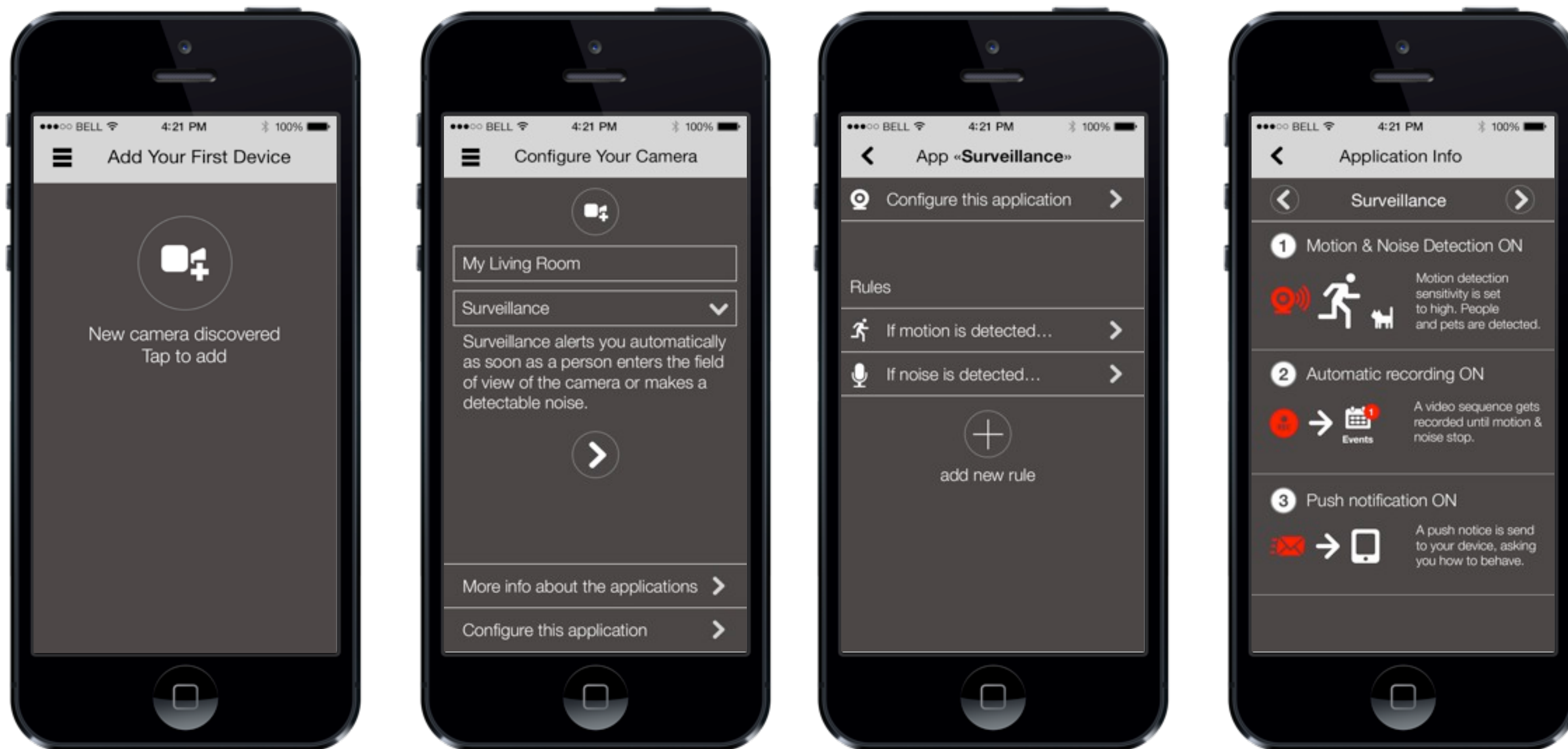


IFTTT Rules
(multiple per Application)

Device Settings










Application Logic

APP – CONFIGURATION



THE APPS (INITIAL IDEAS)



								
Surveillance	Baby-phone	Surveillance	Baby-phone	Care	Alarm Clock	Automation	Presence	Alarm
Customer gets a push notification if motion or noise is detected. Video of the event will be stored in the cloud	Customer gets a push notification if noise is detected and increasing.	Customer gets a push notification if motion,noise, jump of temperature or humidity is detected. Audi track of the event will be stored in the cloud	Customer gets a push notification if noise is detected and increasing.	Customer gets a push notification if no motion or noise after a certain time within a timeframe is detected.	Customer gets a softer „good morning“. The device scans activity and simulates a sunrise before the time to wakeup.	The motion/ audio/ brightness sensors trigger other devices/ actions.	The device is randomly switched on and off to simulate that someone is at home.	Customer gets a push notification if high consumption or turn on/off is detected.

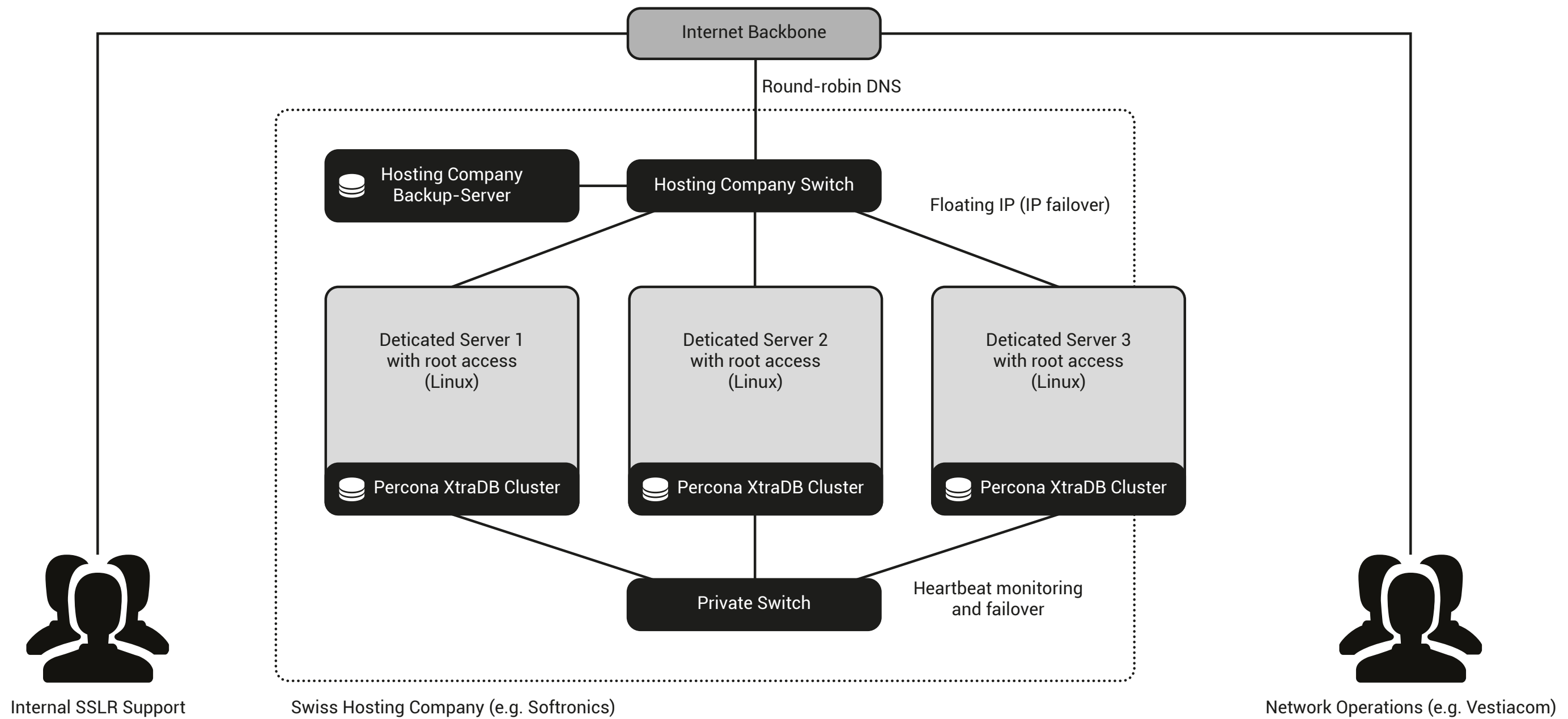
SECURITY

General

- Remote NAS shares the same concept for securing the data exchange (over the internet) between the devices and clients. Remote NAS will be deployed in Stargate and is currently being security audited by Protect7
- Security Audit planned

Stream	Recordings	Local Access	Passwords	Server Access
<ul style="list-style-type: none">. encrypted using either HTTPS or AES128 + ECC-DH key exchange + ECCDSA signature	<ul style="list-style-type: none">. encrypted. keys stored in DB + hardcoded in the server app. not visible for Admin (& Super-Admin)	<ul style="list-style-type: none">. Video stream only available if logged in to the server	<ul style="list-style-type: none">. Camera – random algorithm. User – as strong as he/she defines it (PW requirements – 8 chars with at least one capital letter, on number and one special character)	<ul style="list-style-type: none">. Following OWASP guide
Risks	<ul style="list-style-type: none">. Disk swap @ hosting company + significant reverse engineering effort			

OPERATIONS



PLANNED MILESTONES

14.09.2013 Milestone 1 (version 0.6)	06.10.2013 Milestone 2 (version 0.7)	19.11.2013 Milestone 3 (version 0.8)	01.02.2014 Milestone 4 (version 1.0 RC1)	24.01.2014 Delivery of fully QA'd release (version 1.0 RC2)	Delayed/ Postponed
<ul style="list-style-type: none"> . Camera live monitoring . Full support for Compro cameras (including 2-way audio) . mobile app for iOS only (camera interaction only) . Use cases <ul style="list-style-type: none"> . create user account . delete user account . add Compro camera . view live stream from camera with audio . mute/un-mute audio . control camera's pan/tilt . talk to the camera . request manual video recording . playback of recorded videos 	<ul style="list-style-type: none"> . support for WIFI switch . Use cases (+ all from ver. 0.7): <ul style="list-style-type: none"> . add WIFI switch to the account (assign label and location) . manual control of the switch (on/off) . show switch current power consumption in Watt (if switch supports it) 	<ul style="list-style-type: none"> . support for WIFI AOB . initial support for apps and rule engine . scheduler . initial Android app . Use cases (+ all from ver. 0.8): <ul style="list-style-type: none"> . add WIFI AoB to the account (assign label and location) . manual control of AoB (RGB LED color, play sound) . assign app(s) to switch, AoB and camera . configure app for a device . schedule switch change . schedule app change . schedule scene activation . push notifications delivered to iOS app . motion detection by 	<ul style="list-style-type: none"> . almost all working, but not fully QA'd . left: admin IF changes, coupon management, server less operation . Use cases (+ all from ver. 0.9): <ul style="list-style-type: none"> . access/control devices locally (without server) . register/login with Facebook . see current weather info . automatic update of FW of camera/AoB 	<ul style="list-style-type: none"> . All – except delayed/postponed 	

SSLR IN DEPTH (ON REQUEST)

Architecture / Scalability & Performance

GDC

Devices

Rule Engine (IFTTT)

User Experience / Mobile App

Other details

THANK YOU!