

Internet of Healthcare things

A Platform Approach

Poornachandra Kallare

Connected Digital Platforms and Propositions, Philips

June 2017

Connected digital products

- Global developments in technology are affecting everything around us
 - Cheap connectivity on devices
 - Ubiquitous internet & mobile devices with UI & connectivity
 - Cloud with scalable data storage, processing and analytics



- Connected products are different
 - Services takes priority over devices
 - The need to utilize the power of data through analytics
 - Ecosystems and integration with 3rd parties
 - Continuous updates needed to keep engagement

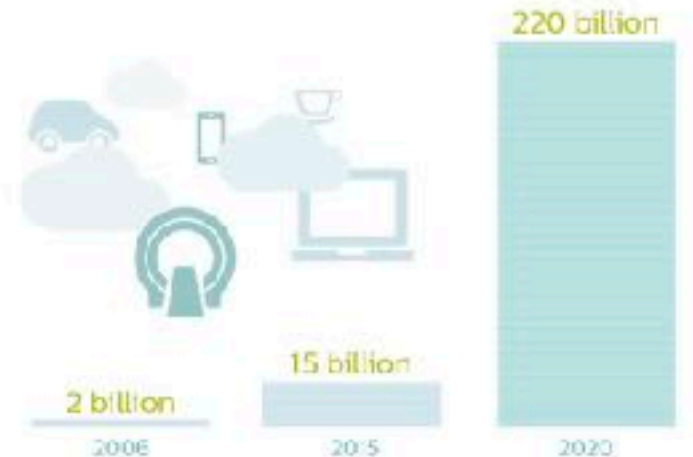


- Products -> Propositions
 - **Digital propositions** consist of **hardware, software and services interconnected by data** and digital content that deliver meaningful smart (through analytics) solutions to a community of customers

Convergence - Consumer Electronics + Healthcare



Thanks to the internet of things



The Health Continuum

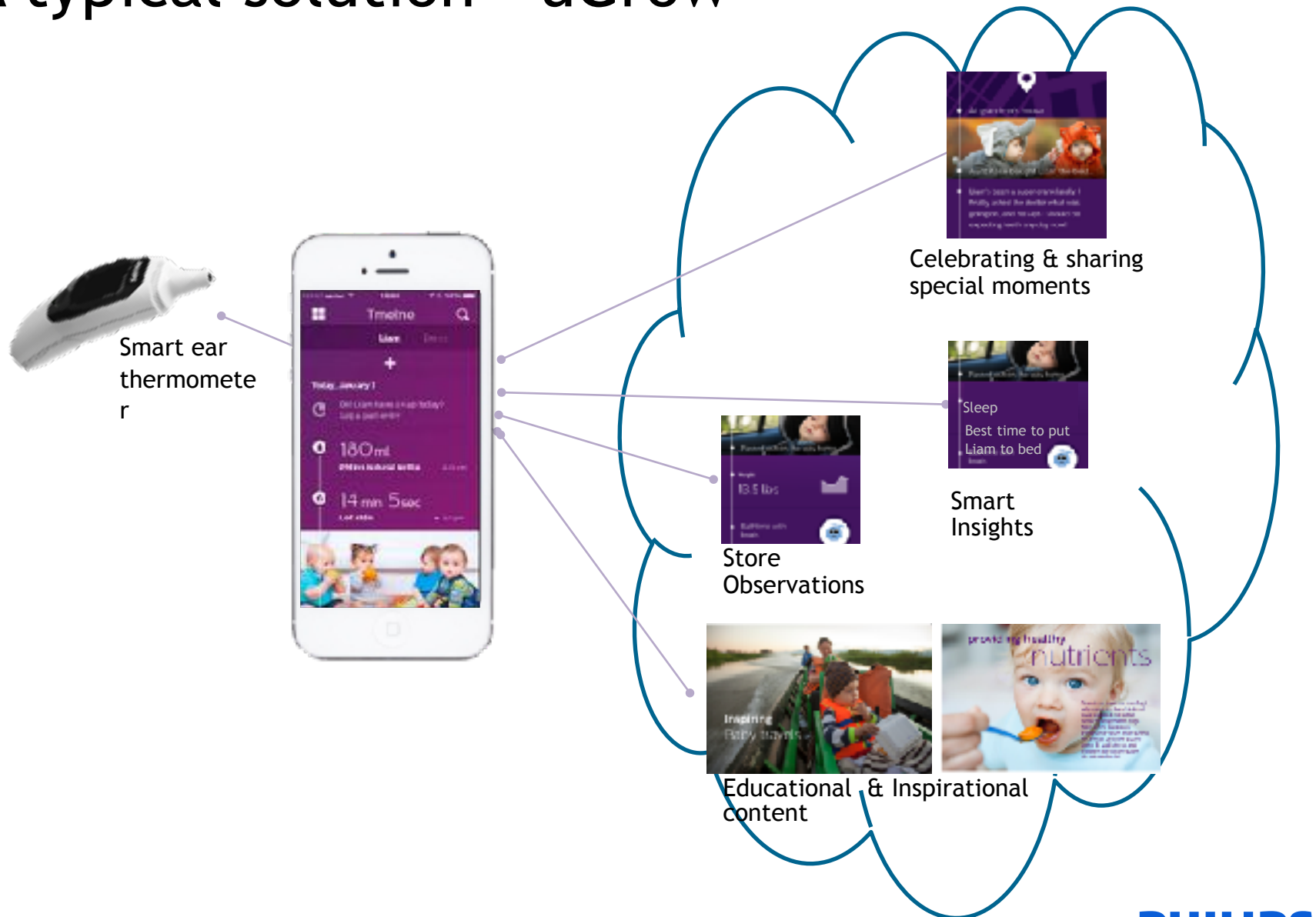


To design and deliver an ecosystem of products, services and solutions enabled through a single, unified Philips user experience across the health continuum.

A Common platform

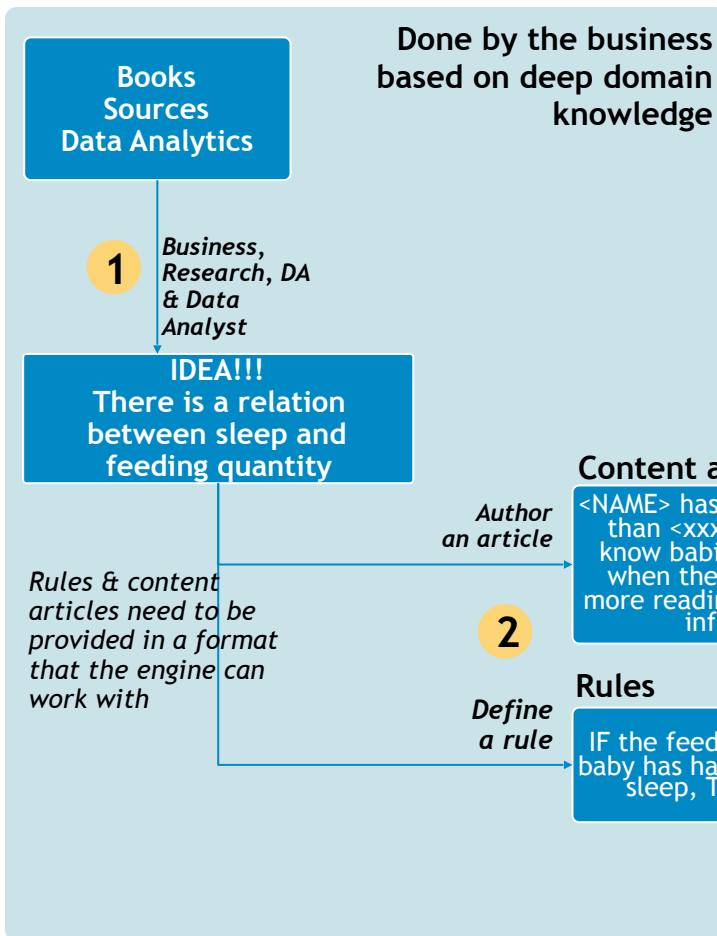
- Single point for user identify and authorization.
- Consistent brand expression, look & feel - DLS
- Combining data from different propositions to deliver the best value (Services, Applications)
- Reduce Time to Market by providing state of the art services, software and operations
- Scale
 - Allow Philips businesses to deliver digital propositions at scale
 - Eliminate redundant development and operations across Philips
 - Reduce (Operational) Costs by economies of scale
- Reduce complexity in security and compliance efforts
 - Do it right. Once !

A typical solution - uGrow

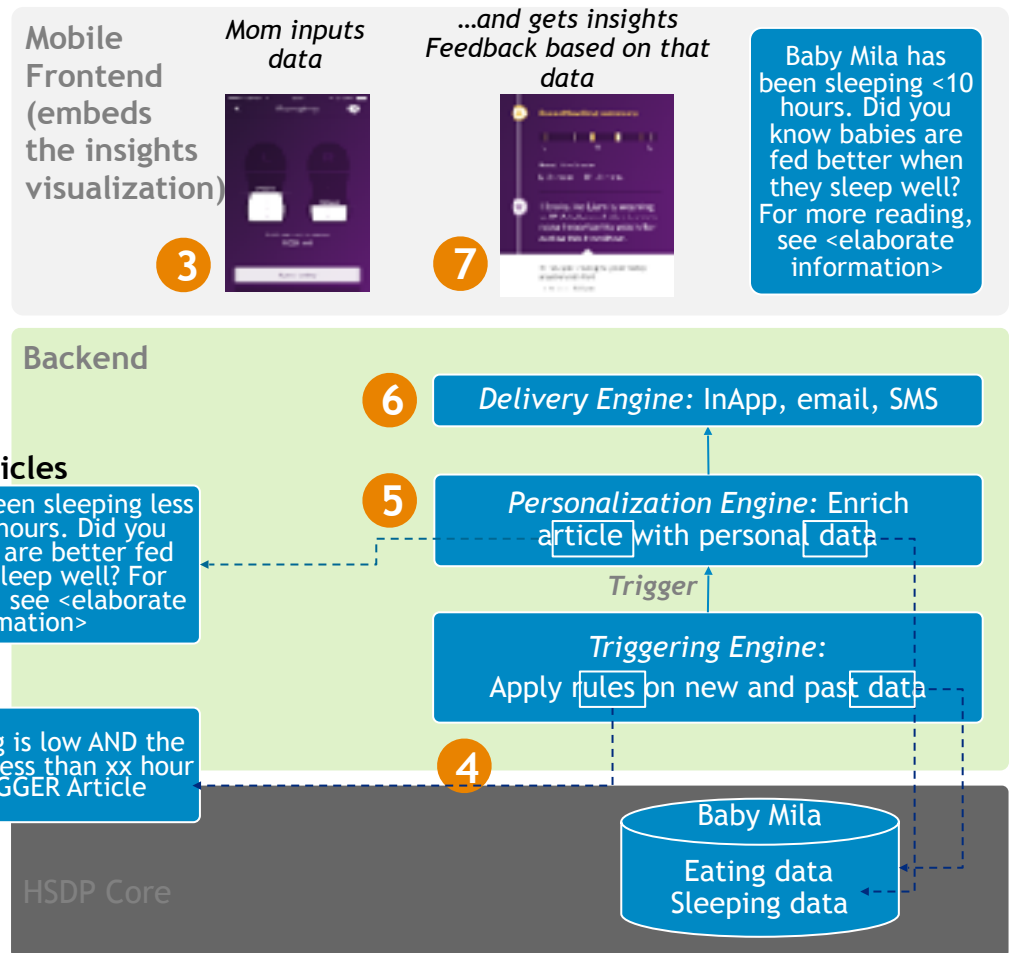


uGrow - Under the hood

Process to Discover / define insights



Operational product



Building Blocks can be many things



What is personal data?

and sensitive personal data...

Personal data is any information on the basis of which you can directly or indirectly identify an individual.
The Philips Privacy Rules become stricter when sensitive personal data is concerned.

Personal Data



Birth Date



Department



Profile



IP addresses



Preferences



Address (business
as well as private)

Sensitive Data



Ethnicity



Health



Race



Sexual preference



Religion



Criminal History



Evaluations and
Competences

What can we do?

1 Practice Privacy By Design

Be proactive. Ask important questions and embed privacy measures throughout the lifecycle of your product or service.

2 Communicate Openly & Effectively

Have a comprehensive and transparent privacy policy covering all of your data collection, sharing, and use practices. Use clear and simple language.

3 Make Your Privacy Policy Easily Accessible

Don't make users search for your privacy policy—make it prominent and easy to find.

4 Use Enhanced Notice

Don't surprise users—have respect for context. Use enhanced notice in situations where users might not expect certain data to be collected.

5 Provide Users with Choices & Controls

Empower users. Allow them to choose and control the way their data is collected and used.

6 Secure Your Users' Data!

Always use appropriate end-to-end security measures to protect user data.

7 Ensure Accountability

Make sure someone is in charge! Designate a privacy guardian or make sure to explicitly assume the responsibility yourself.

What are the main principles....

- ✓ Transparency
- ✓ Consent (if needed)
- ✓ Third party data processing



Provide transparency

Privacy notice....

Privacy Notice

When people share data, they need to know how their personal data will be used.

A Privacy Notice must explain:



- The **identity** of the organization who is responsible for processing the personal data



- The **type of personal data** we collect and the **purpose** for collecting that data



- **Security measures**



- Which category of **third parties** you make use of, if any, and for what purpose



- The **Rights of data subjects** including
 - Access to his/her personal data & info concerning how the data is used
 - The right to update his/her personal data that is in your hands
 - Blocking/updating potentially inaccurate data
 - Erasing data that is not lawfully processed
 - The right to object to direct marketing



- **Other Important Issues** affecting consumers' personal data

How to provide a Privacy Notice:

- You must **always** provide a Privacy Notice
- The Privacy Notice must **always be available and easily accessible** at a digital touchpoint
- It should be available to read **before processing** takes place with the option for later review.
- It does not need to be accepted.

Obtain consent

Get permission when needed...

Consent

In some cases you are only allowed to process personal data if you have acquired **prior consent** from the individual

Where consent is always required:



- For special categories of (personal) data



- Where you intend to process the consumer's **location data**



- Where you process **sensitive data**, such as health data, race or ethnic origin (including photos or videos), religion, membership of a trade union, sex life, criminal offences/records, social security numbers, financial data



- Data collected by means of **cookies or similar techniques** such as beacons, pixels, biometrics



- Usage data of a phone, application, mobile device, or machine



- When personal data is processed for **certain purposes**



- Data used for **direct marketing**



- (Combined) data used for **profiling** (personalized and individually targeted messages) or **behavioral targeting or predictive analytics**



- In some cases, where data is **transferred outside the country** (eg. China)



- When a touchpoint is **directly targeted to children** (here you require the consent of a parent or guardian)

What must happen when you are asking for consent:

- Consent must be obtained **before collecting** any of the consumer's personal data
- The consumer can only consent to the processing of personal data after (s)he has been **informed**
- The consent needs to be **specific** and based on appropriate and easily understandable information



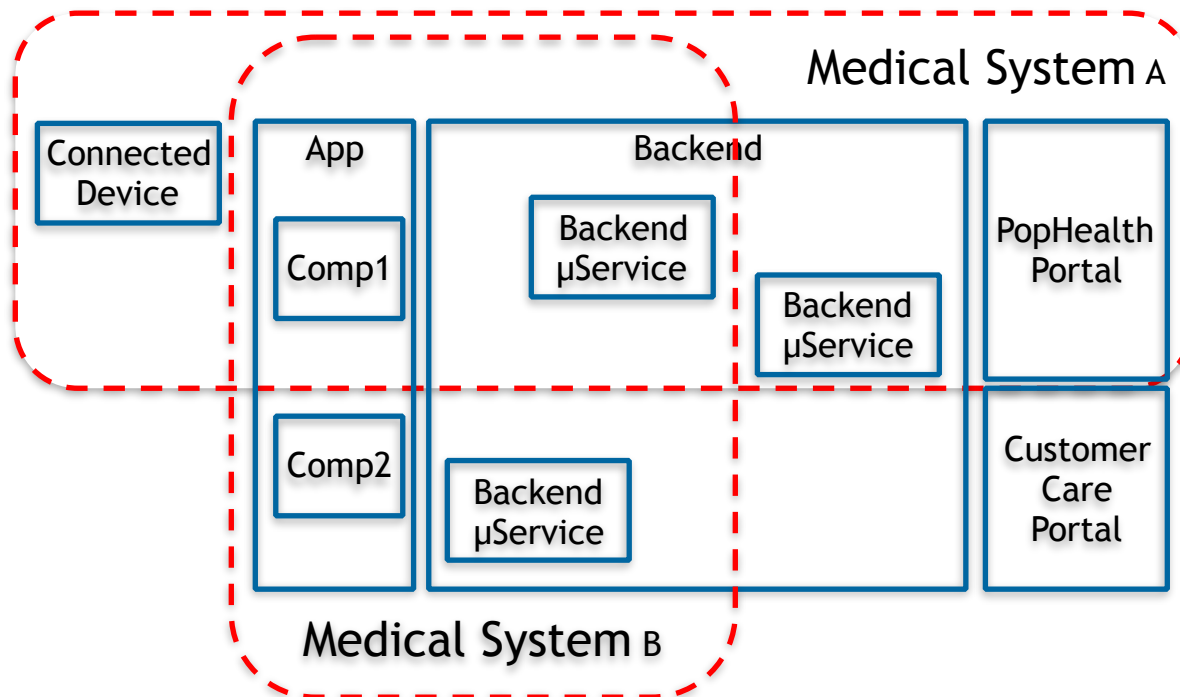
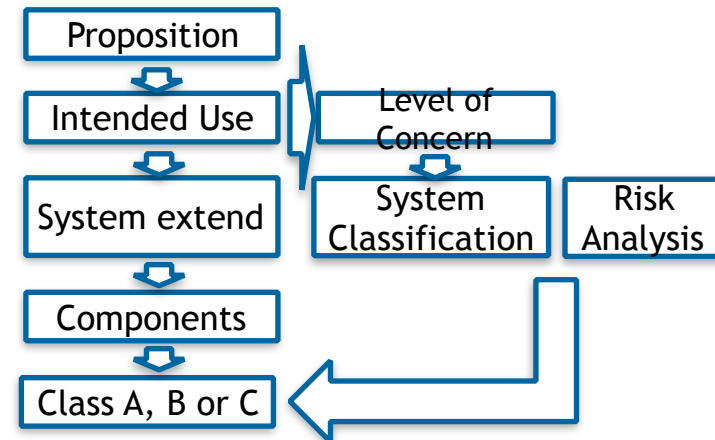
- Consent is an **active choice**. The consumer must consent by **actively** indicating his/her wishes (eg. unticked opt-in box)



- Consent needs to be **freely given**. The consumer must not be deceived or coerced into giving consent

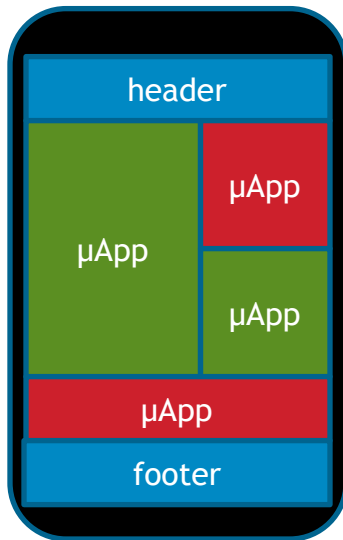
Medical device classification

- Class A: No injury or damage to health is possible
- Class B: Non-SERIOUS INJURY is possible
- Class C: Death or SERIOUS INJURY is possible

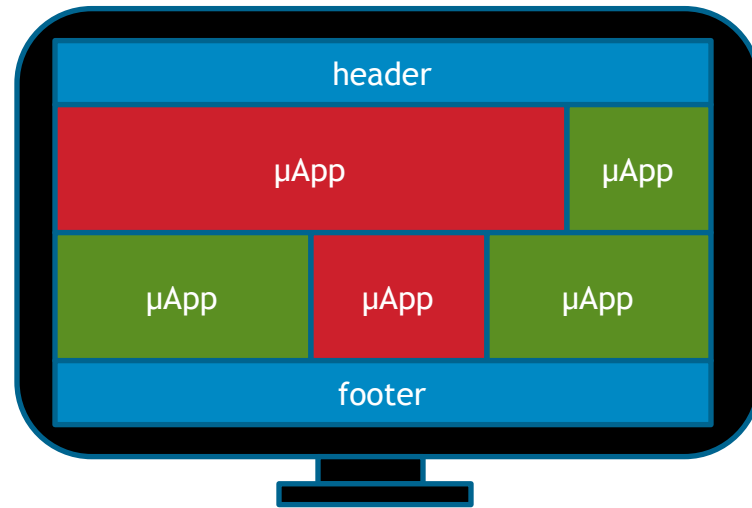


Frontend building blocks - μ App

e.g. Mobile Patient Engagement App

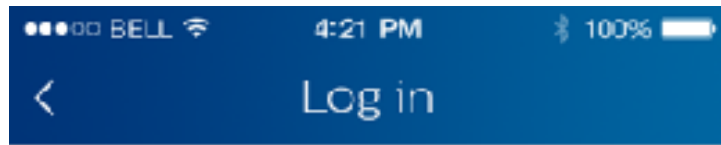


e.g. Browser-based Care Provider Dashboard




- Applications are composed of discrete, loosely coupled, semi-independent building blocks
- Applications use **standard** as well as **domain-specific** building blocks
- Micro apps are the front-end portion of such building blocks
- Other portions reside in micro services running in the back-end
- Micro apps are composed in an application framework (a 'shell') that provides client-side infrastructure for e.g. communication, logging, layouting, navigation...

μApp Example - User Registration



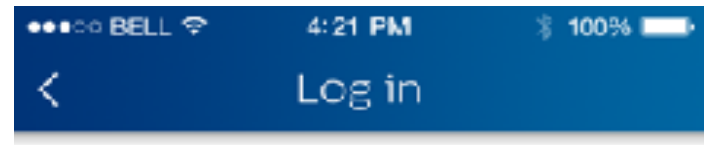
Log in with Philips account

Your email or phone number

Enter password 

Log in

Forgot Password



Almost done!

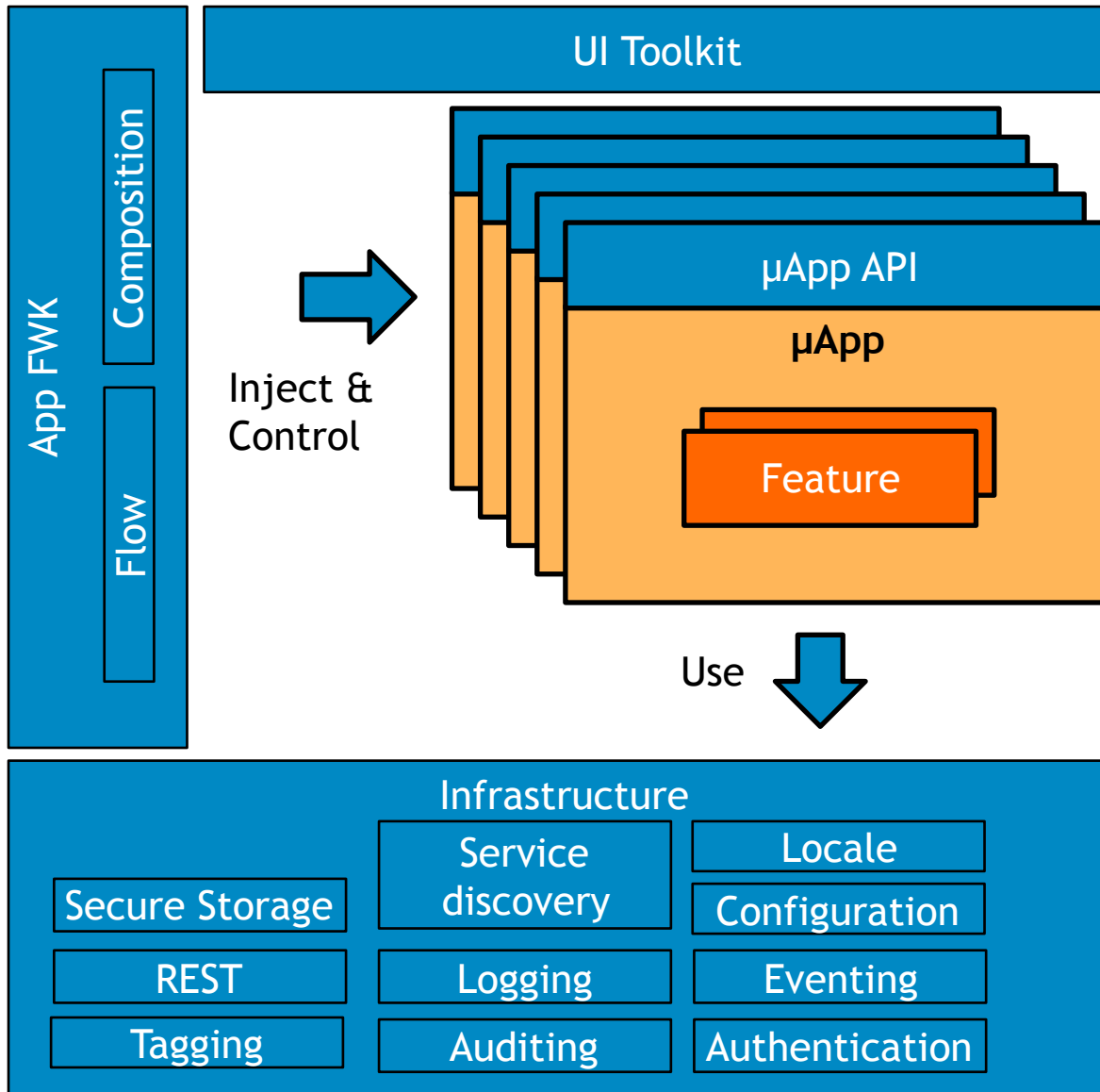
Your email or phone number

I accept the app's Terms & Conditions ☒

Receive promotional communications of Philips based on my preferences and online behavior
What does this mean? ☐

Continue

Composability - μ App Framework



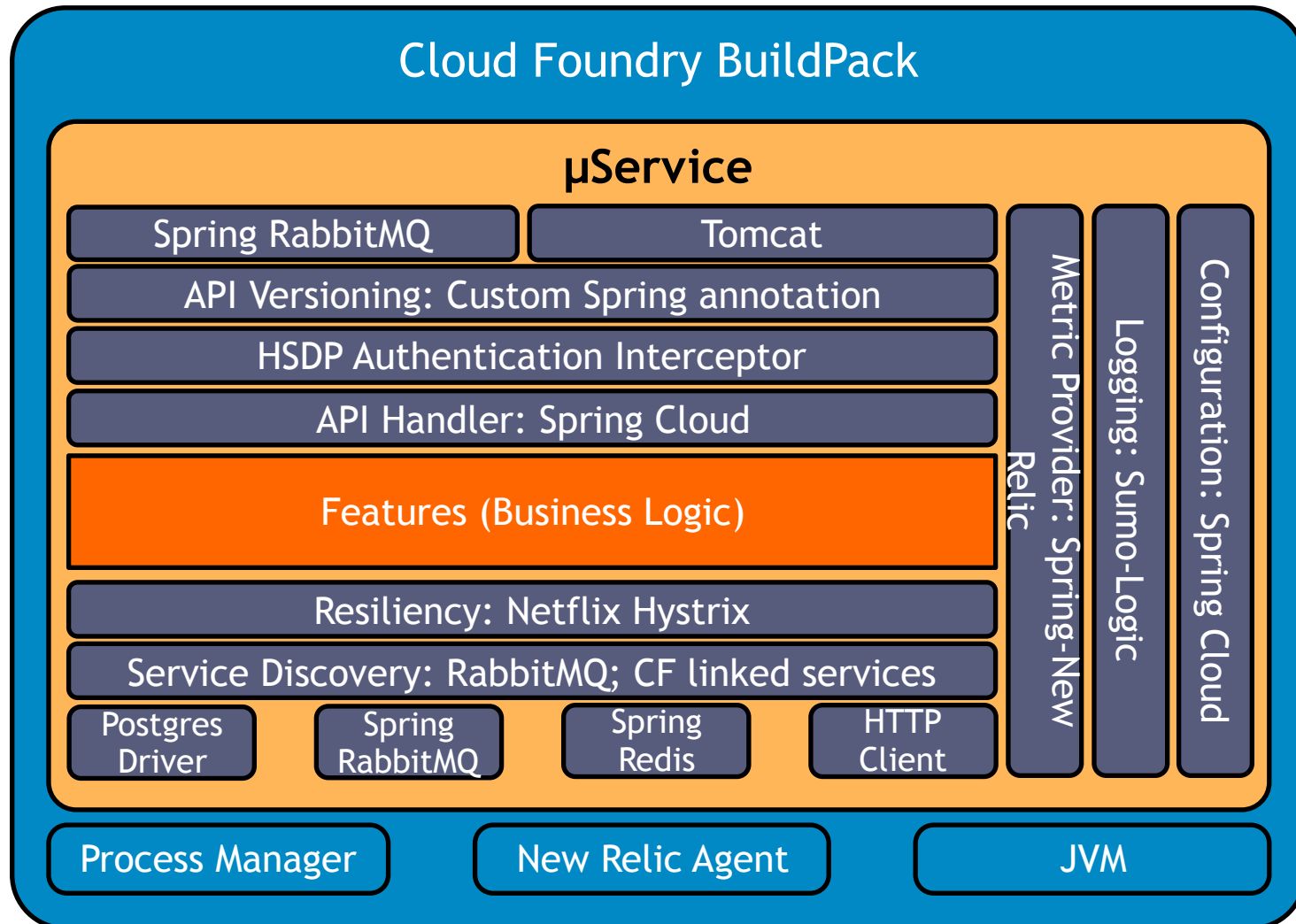
Key Challenges - Mobile

- Uniform logging format
- Tagging of user actions
- Managing configuration options
- Determining user locale
- Audit trails
- Consent
 - Explicit/informed consent
 - Storage of consent

Key Challenges - Mobile

- Mobile devices are open
 - Not “controlled”
 - We store personal health information
- Security
 - Use Android key store and iOS keychain
 - Randomly generated encryption key pair stored in the keychain/keystore
 - Data encrypted using key pair
 - Secure database
 - iOS Protection classes
 - Detection if lock set (> iOS9)
 - DeviceOwnerAuthentication
 - Android SqlCipher
 - Storage of “secrets” (Example: API signing keys)

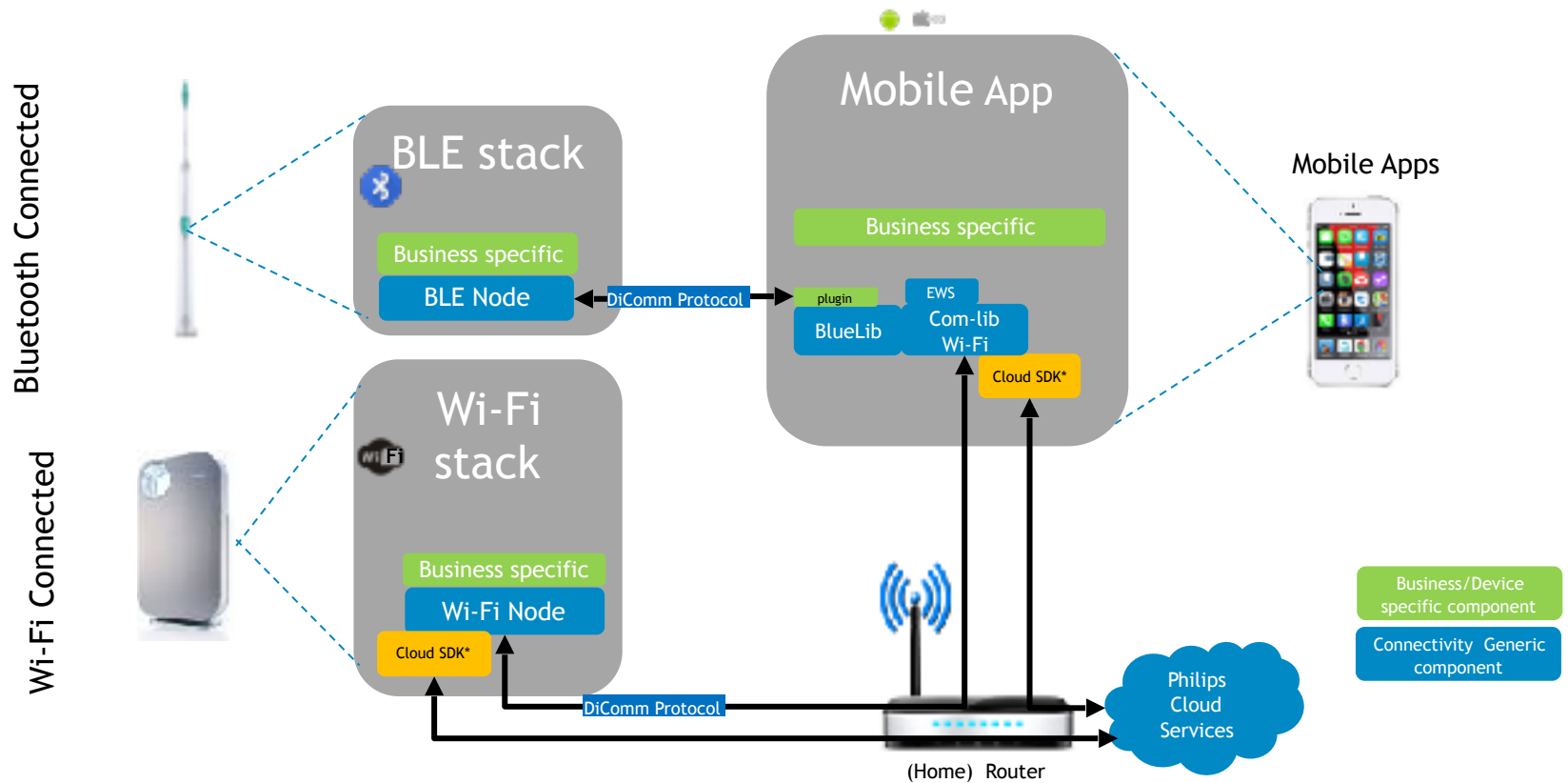
Backend building blocks - μ Services



Key Challenges - Backend

- Fast deployment while staying compliant
 - Be smart in defining the boundaries of your service
 - Separate out the algorithms from the service
 - Example: Rules vs rule engine
- Have the storage locations of the personal data been determined?
 - Routing the right user to the right data store
 - Data residency regulations
- Right to delete data
 - Do you have a system in place to ensure all relevant data is deleted when a user wants to?
- Sharing & consent, access control, tenants
- Data model & interoperability
 - FHIR (Fast Healthcare Interoperability Resources)
 - ILS (Information Language System)

Device Connectivity Architecture



Device connectivity

- BLE
 - Standard BLE profiles wherever possible
 - Thermometer profile
 - Combination of profiles
 - Multiple sensors
 - Custom protocol in case of complex custom devices
 - Secure software update
 - DICOMM
- Wi-Fi
 - SSDP for discovery
 - HTTPS for communication

Key Challenges - Device connectivity

- Easy to DDOS yourself
 - Devices are not random
- Bluetooth low energy connectivity on Android phones
 - Many detailed deviations from BLE Standards
 - CDP2 developed a library to deal with many of those issues
 - Have to test products with BLE connectivity on many mobile devices → Mobile test farm
- Security
 - BLE transport level encryption
 - BLE protocol important based on use case
 - JustPairing works acceptable for stationary devices
 - Example: Tooth brush
 - Pin/Password mandatory for mobile devices
 - Health watch
 - Certificate pinning
 - Part of the pairing process for Wi-Fi devices

Device connectivity - Securing a device

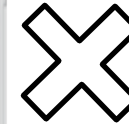
- Can the firmware of the Device be updated?
 - Are the firmware update files encrypted
 - Are the firmware update files authenticated /signed
- Does the Device store unencrypted Personal Data
 - Is the integrity of stored Personal data checked
- Does the Device store Passwords
 - Are the stored Passwords encrypted
 - Alternative are the stored Passwords obfuscated
 - Are the passwords the same for all devices ?
- Does the Device store Secret Keys
 - Are the stored Secrets Keys encrypted
 - Alternative, are the stored Secrets Keys obfuscated
- Are the Device's debug i/f disabled for end-user access
- Are the Device's command i/f disabled for end-user access
- Does the Device communicate unencrypted Personal Data
- Does the Device communicate unencrypted Secret Keys
- Does the Device communicate unencrypted Passwords
- Does the Device support logging
 - Are the logs checked for Personal Data
 - Are the logs checked for Integrity

Platform Life Cycle - Combinatorial complexity

Firmware versions



App versions



Android Devices

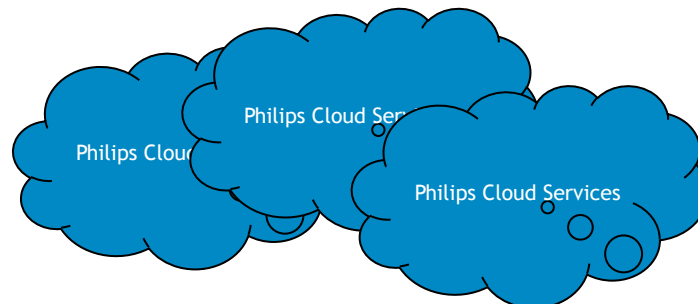
Android Versions

iOS Devices

iOS Versions



Backend versions



Does it make sense to build platforms?

- It depends
 - Scale makes it worth it.
- Think critically if something is a platform feature
- Build/Mature in the context of a lead solution
- Stick to architecture rules/guidelines
- Harvest !

