TrustedCare
Be Empowered

Move Health Data Forward Challenge
Prototype and Pilot (Phase II)

ARM

Enabling seamless integration of Care Provider in ACO model

Accountable real-time patient TeleCare management

This presentation outlines the prototyping of TeleCare devices to enable ACO providers

Goal

*Extend HEART spec to enable new "accountable care devices" to be involved in shared risk/saving ACO payment model**

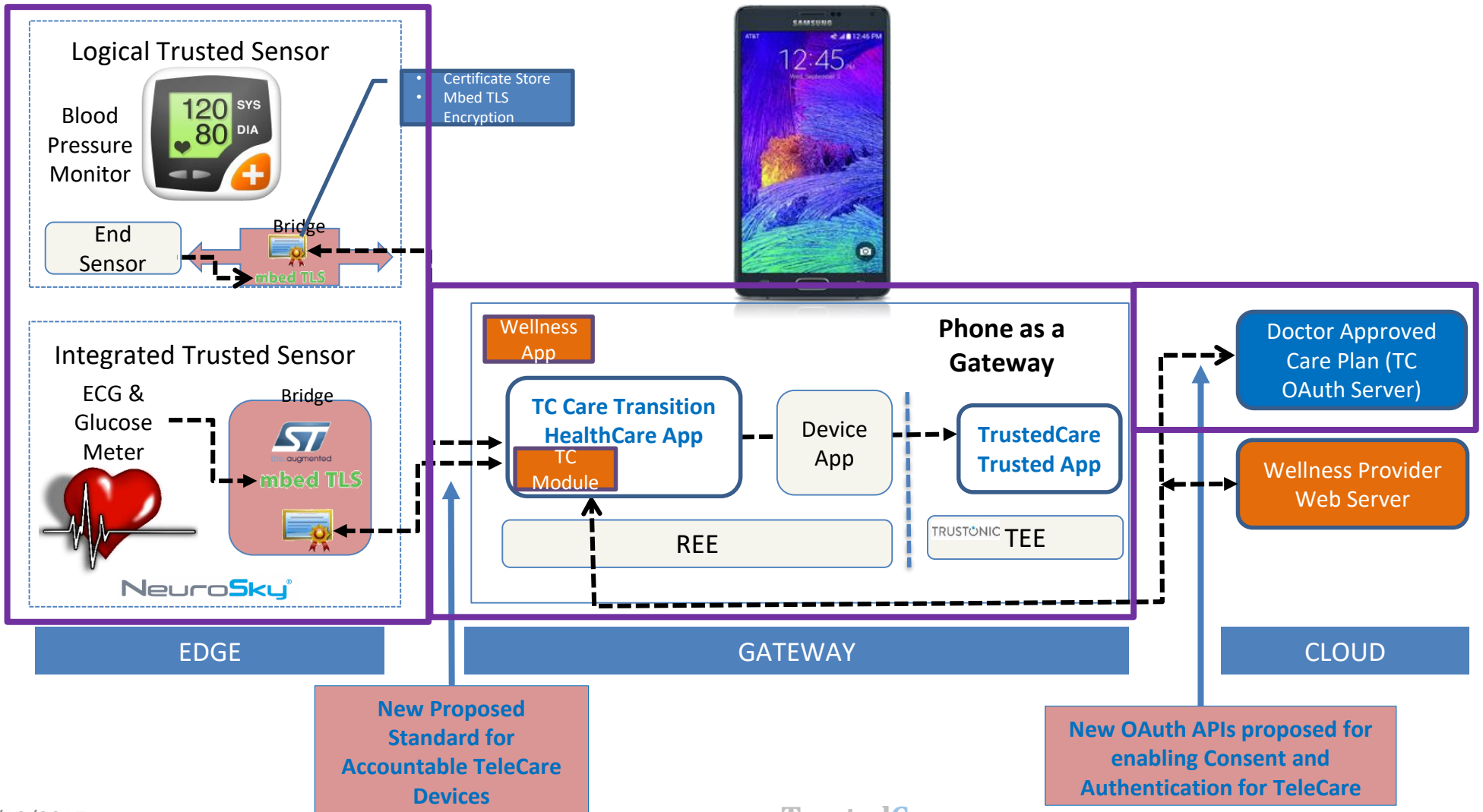
Outcome

- *Enable data to be forwarded to multi-parties with patient consent*
- *Enable **auditable** trail of Care Provider services, Patient Compliance*
- *Demonstrate this can be scalable to multiple parties and devices*
- *Enable outcome based payment authorization for participants*

**TrustedCare is engaged with ARM in their efforts to develop a new device level standard called OpenMedReady to enable a new category of telecare devices for Accountable Care*

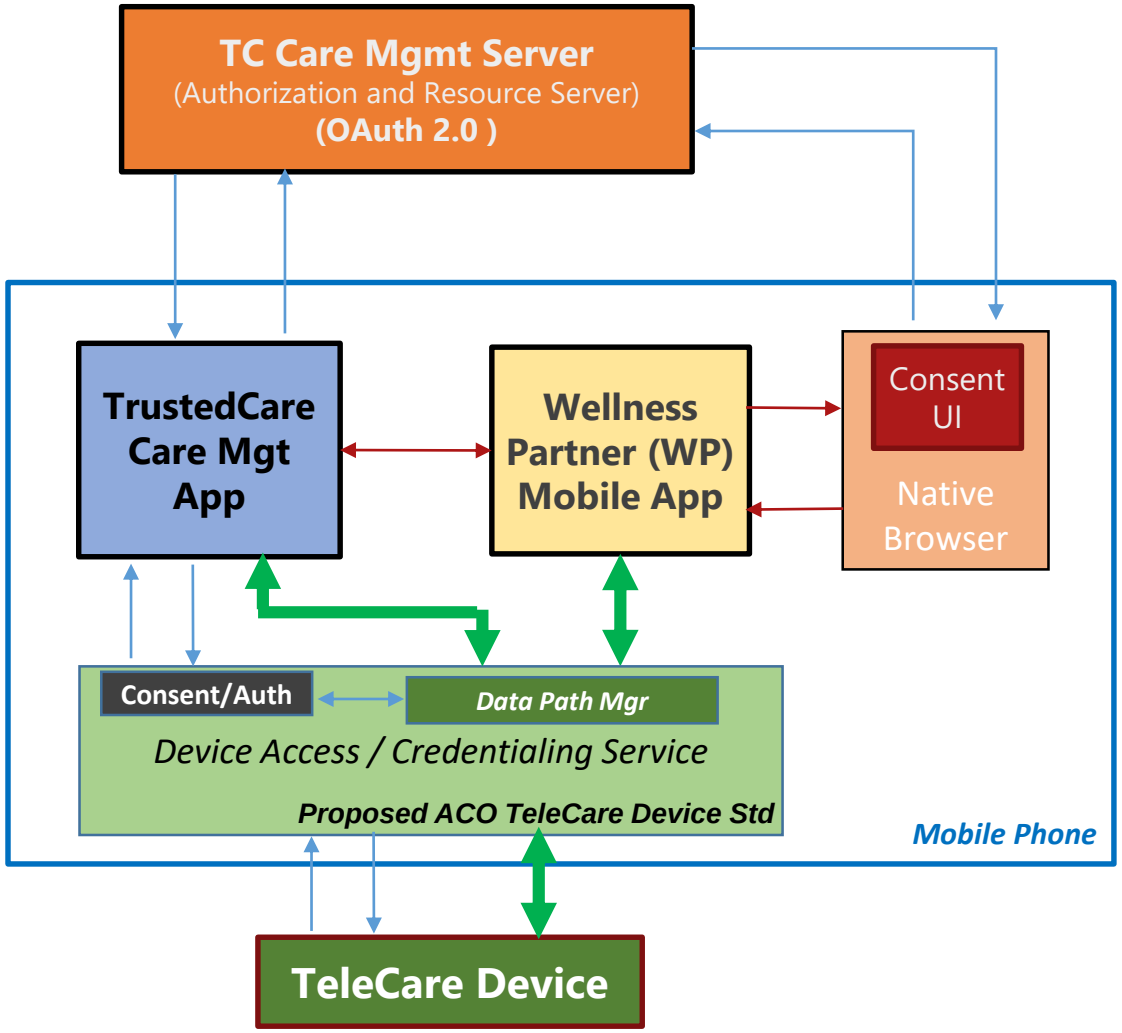
Recall: The Overall Product Schematic

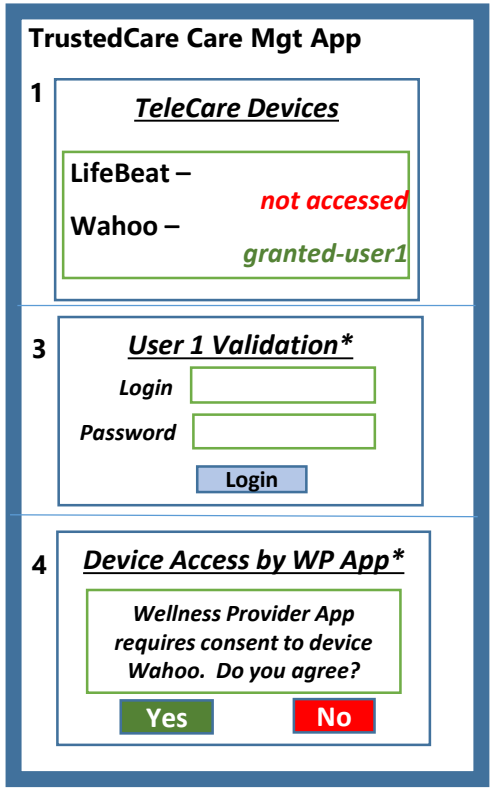
Prototyping Effort to demonstrate Consent/Authorization of Wellness App by Care Mgt App



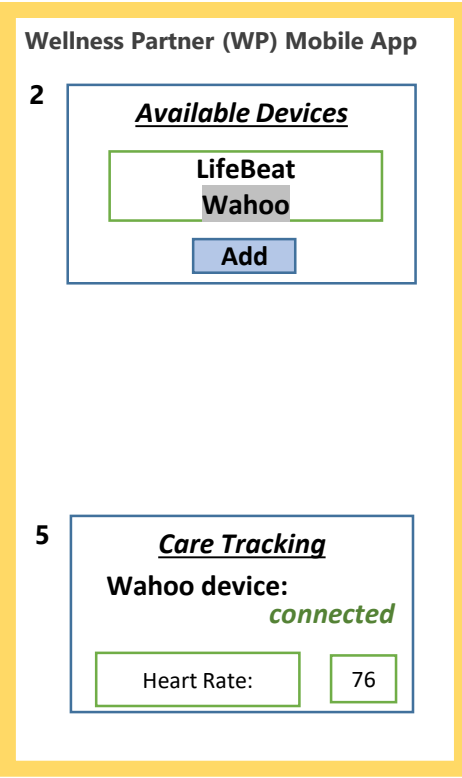
Components involved in Prototyping effort

Prototype Schematic, App Components & Sequence



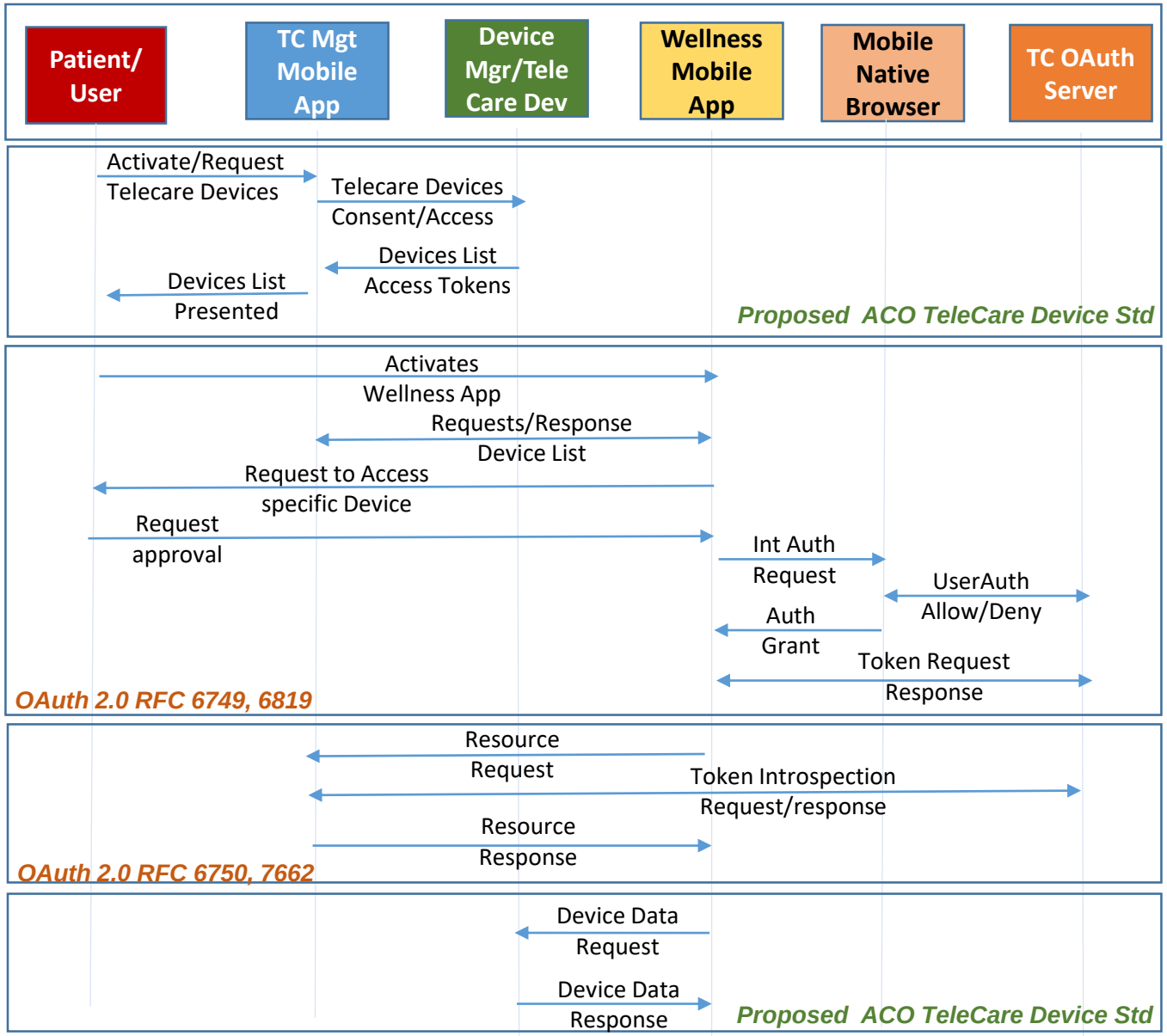


*Via Native Web Browser



1. *Care Management app can manage published Telecare devices (screen 1)*
2. *Wellness Provider app asks & gets the list of devices from TC Care Management App (screen 2). It then asks for consent to use one of them by launching web browser to TC OAuth Server.*
3. *The consent request is sent to TC Care Management server (OAuth server) via native Browser for validation (screens 3,4), token is sent back to WP app*
4. *Wellness Provider app then passes the token to TC Care Management App on the phone*
5. *Upon receiving and validating the token (via Token Introspection), TC Care Management app grants access to device to Wellness Provider app (screen 5)*

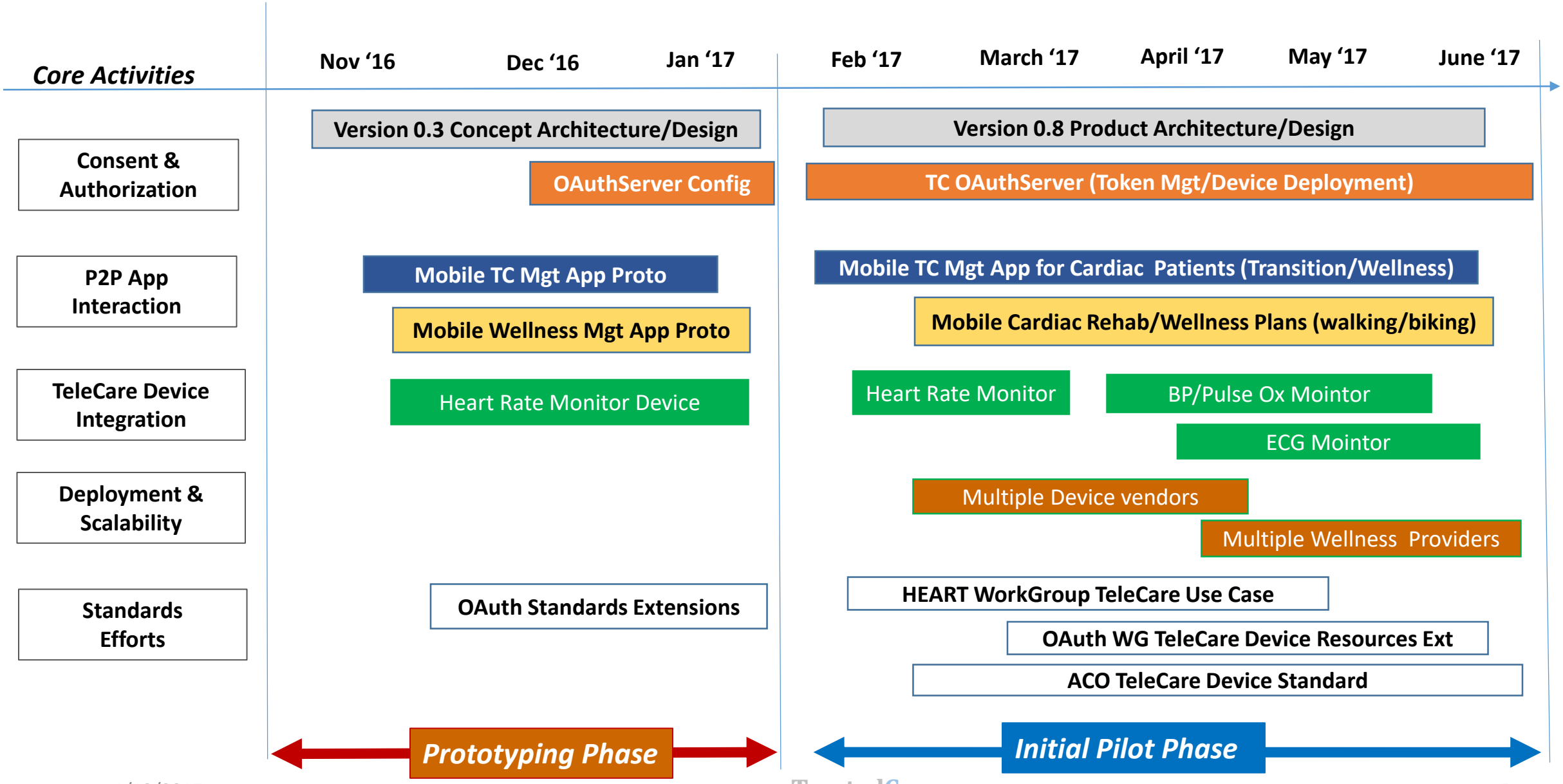
Prototype Workflow and Tasks



Key Prototyping Tasks:

1. Care Mgt App (Resource Owner) claim Telecare Device Access/Control
2. Wellness App (Third Party) Requests Telecare Resource Access Authorization
3. Wellness App Requests Access to TeleCare Device via Authorization Server
4. Wellness Devices Access TeleCare Device with Audit Trail

Product Prototype & Pilot Timeline and Activities

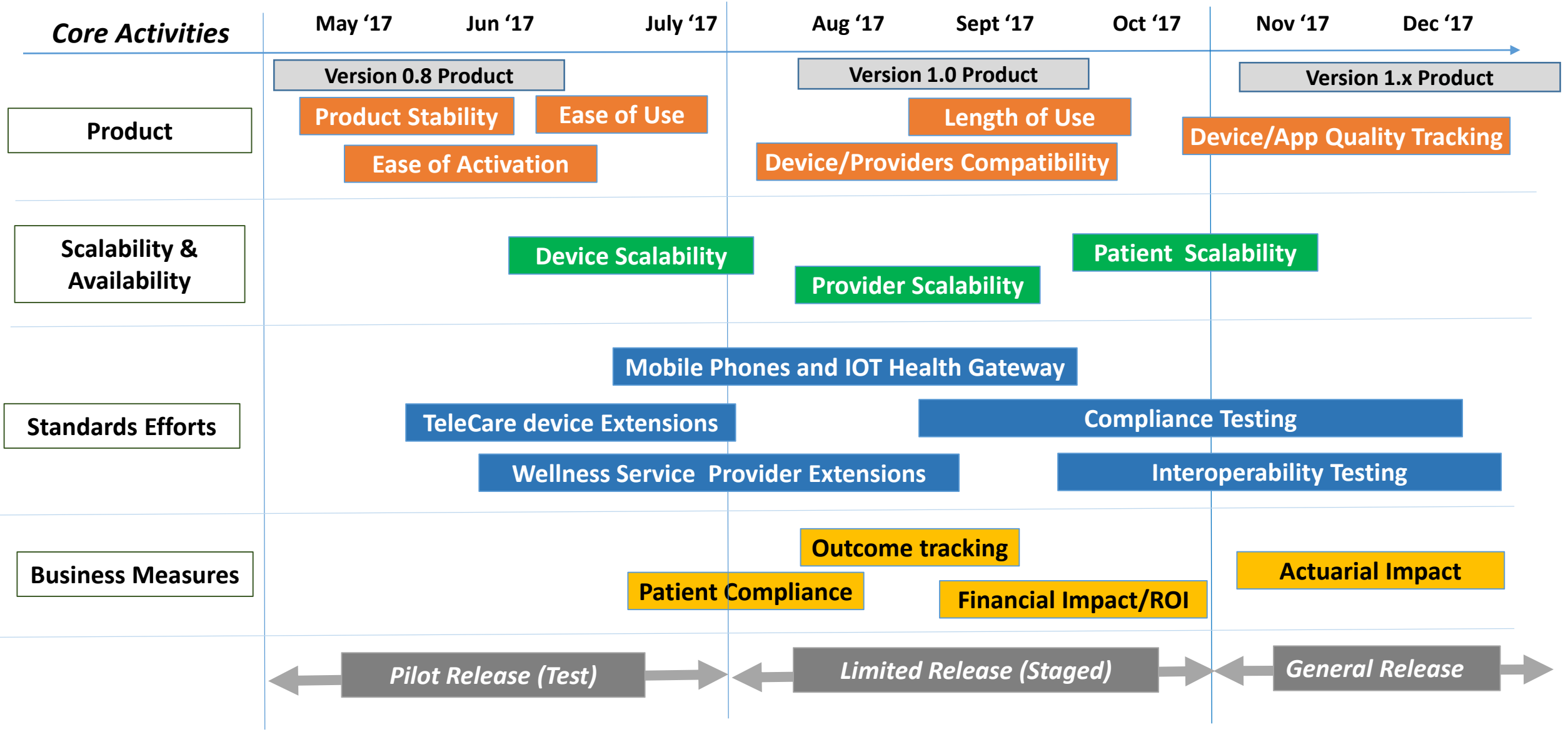


Product Prototype & Pilot Resources and Budget

Prototyping Activities	Resources	Sub-Total
Product Concept Arch/Design	$7K	$7K
Mobile Care Mgt Proto App	$5K	$5K
Wellness Mgt Proto App	$4K	$4K
Total		**$16K**

Pilot Activities *(Planned)*	Resources *(Estimates)*		Sub-Total
	Personnel	*Infrastructure*	
Authorization/Consent Server, Token/Certs Mgt	$25K	$10K	$35K
Mobile Care Mgt App Dev	$30K	$5K	$35K
Wellness Mgt App Dev	$25K		$25K
Pilot Project Launch *(Devices, Device Mgt, Project Manager)*	$30K	$50K	$80K
Care Management *(Case Management)*	$25K		$25K
Validation & Service & Support	$20K		$20K
Standards Effort	$20K		$20K
Total			**$240K**

Proposed Production Activities and Timeline



Extensions to Oauth, HEART WG, ACO TeleCare Device Standards

- **Emerging Usage Models for HealthCare**
  - New use case for OAuth / HEART with the use of smart phone apps and IOT Health Gateways, which will require new scope values to be defined.
  - Growth in Home Health Gateway IOT devices to enable “Care-in-Place” needs to be addressed
  - Need for Audited HealthCare for Smart Contract Payments in ACO paradigms
- **Infrastructure & Resource management**
  - Use of resource request locally from one app to another one in a secure fashion rather than the classical Web/native app OAuth usage. This requires a secure inter-process communication technique.
  - Use of resource server on the medical device, which raises questions regarding authentication and authorization. This requires a resource request from the smart phone to the medical device via Bluetooth Low Energy and the definition of the protocol interaction.
  - Improved protection of medical data on the smart phone by utilizing Trusted Execution Environment technology.
- **Smart Phone and Home Health Gateway connectivity to medical devices***
  - Improved security against unauthorized access to resources on medical devices by other apps on the smart phone by using application layer security (in addition to Bluetooth Low Energy link layer security) using TLS.
  - The following items need to be explored for the interaction between the smart phone/ IOT and the BLE device:
    - Version of TLS and placement of roles.
    - Performance and code size for security functionality on medical device
    - Additional hardware requirements for added security
    - Key provisioning technique for management of long-term credentials and device management.

**Will be address as part of the ACO Telecare device standard*

Summary

In this endeavor TrustedCare and ARM are prototyping the capability of telecare devices to become “plug-and-playable” in the Accountable Care shared risk/saving paradigm. We will demonstrate that by leveraging the HEART WG standards a new level of Care Management will be achieved that can be authenticated and audited via patient enabled, consent driven access to data. In addition, enabling patient choice of wellness provider services would drive adherence to care regimes that promises significant improvement in patient wellness.

In addition we have identified areas were the HEART WG use cases and OAuth resource scope need to be extended and the ACO TeleCare device standard needs to cover.