



Trusted Architecture for Securely Shared Services

Healthcare integration trial demonstration

Tom Kirkham
University of Nottingham


**“Current and emerging challenges of eHealth –
privacy, law, ethics, governance and beyond”**

eHealth Workshop Middlesex University, London UK
16-17 June-2011

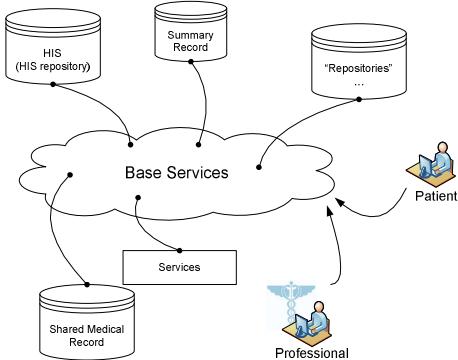
 *TAS³ Consortium*

Integration Trial

eHealth Environment

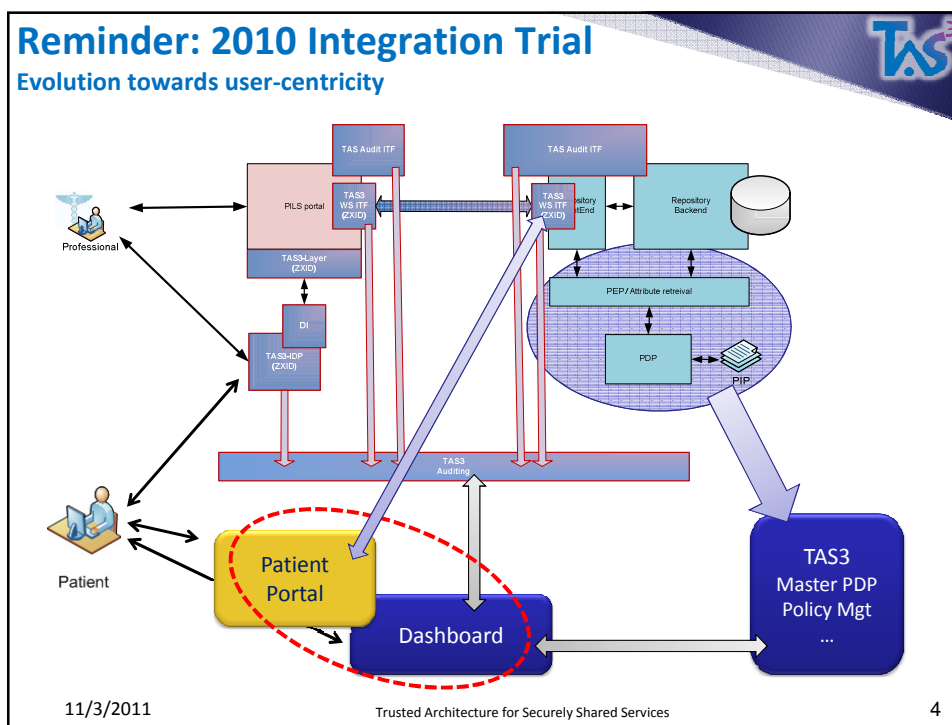
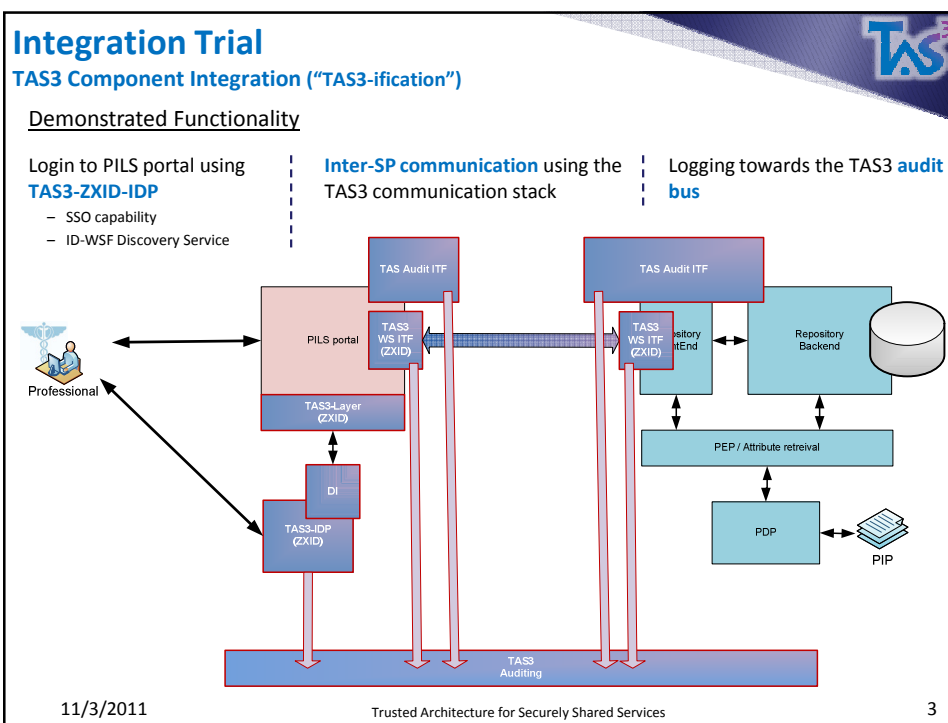


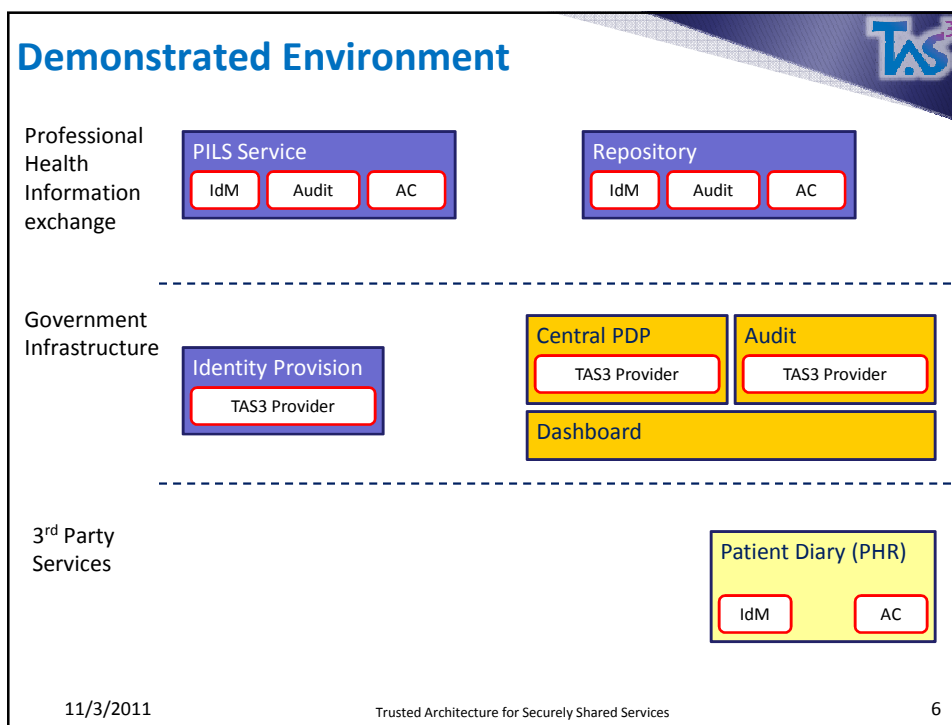
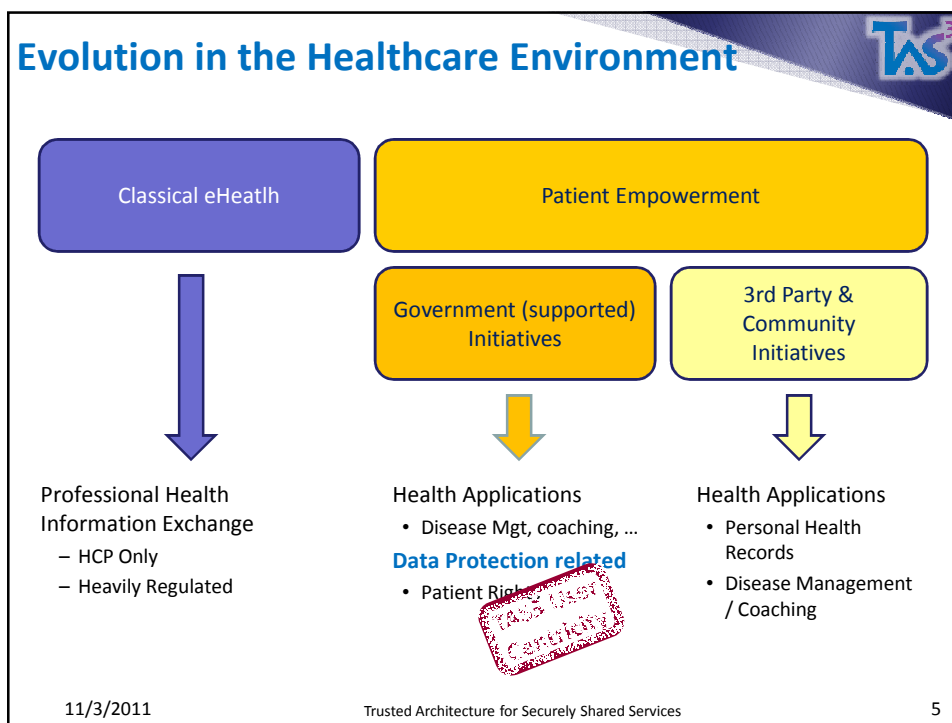
- eHealth environment
 - Data exchange within a Registry - Repository architecture
- Legacy Application
 - Belgian situation
 - Data-format: KMEHR
 - Identifiers: INSS, RIZIV-INAMI
 - PILS Portal (“search”)
 - Patient Information
 - Location Service
 - Repositories
 - Hospital “result servers”
 - Summary Servers
 - ...



The 2011 Trial builds on this...

11/3/2011 Trusted Architecture for Securely Shared Services 2





User-Centricity: Centralized Policy Decisions

Services are responsible for formulating correct AC requests to central PDP

Services therefore:

- Need to be aware of **scope of the central AC Decisions**
- Need to speak “**central PDP security vocabulary**”
- Needs to appropriately **combine central & local access decisions**

The dashboard allows end-users to specify their data protection policies in a user friendly way

- Dashboard **combines user-preferences with the globally accepted domain policy** and saves it as a PDP interpretable policy

11/3/2011 Trusted Architecture for Securely Shared Services 7

User-Centricity: Centralized Policy Decisions

Personal Policy
XACML Target: “Resource about Patient”

Domain restriction taken into account

OPT-OUT

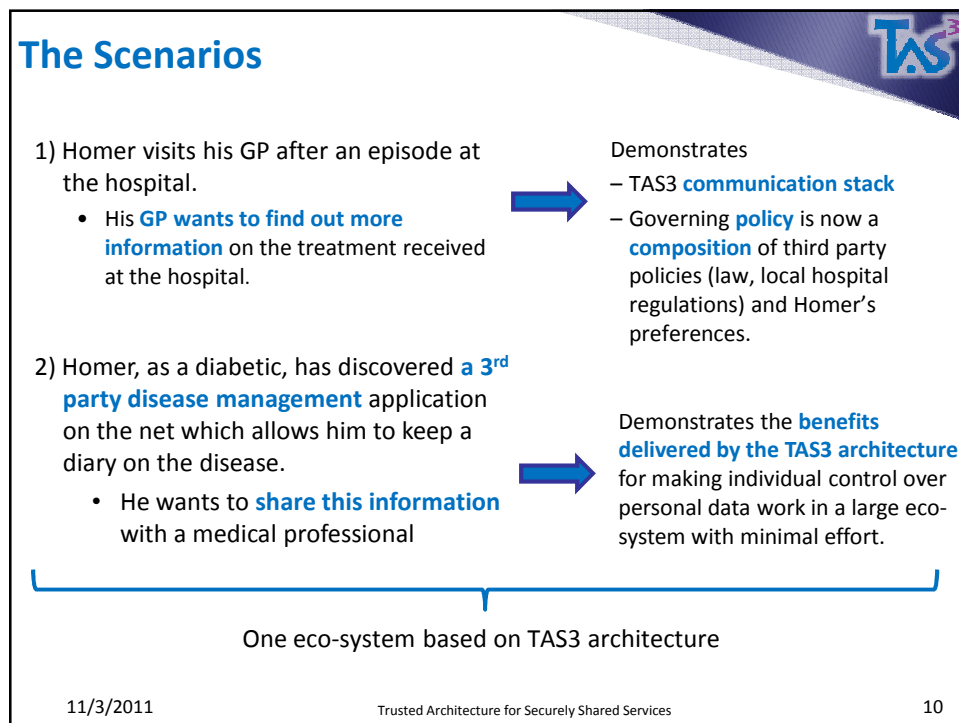
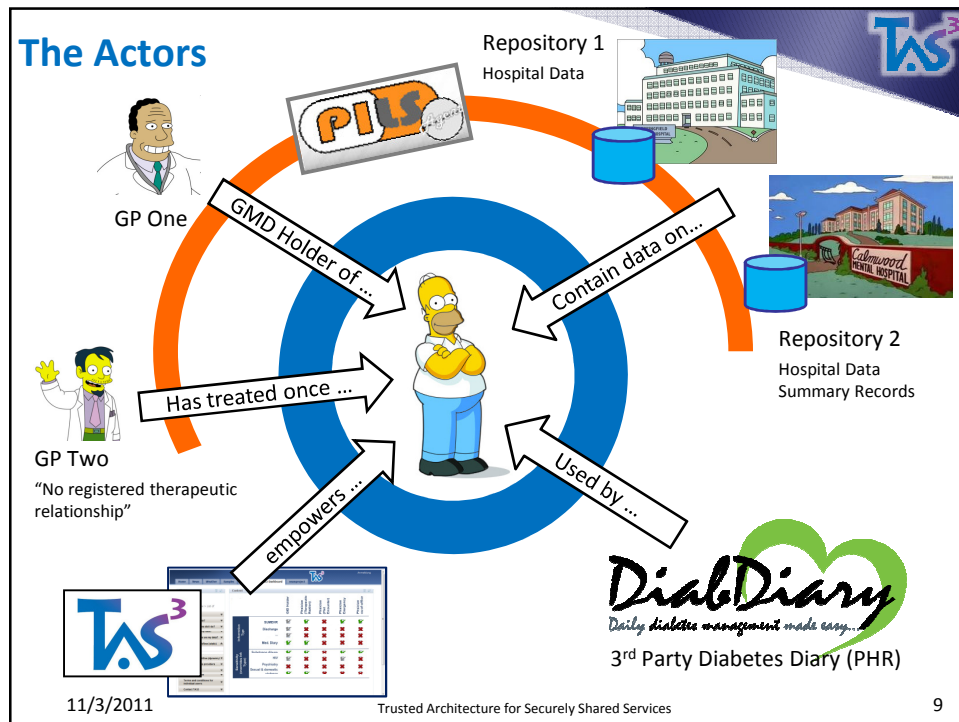
OPT-IN

Deny Overrides

Permit Overrides

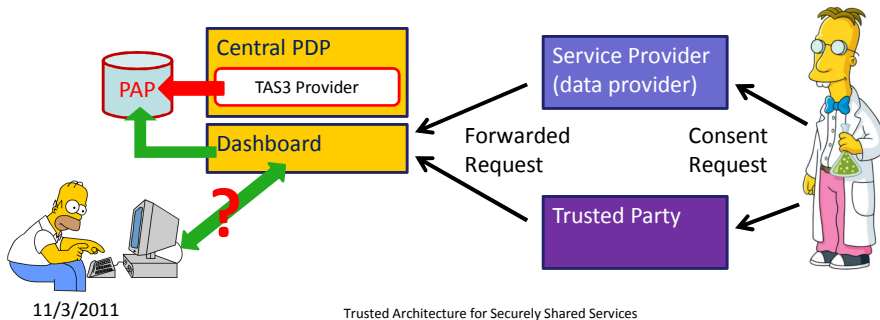
Deny All

11/3/2011 Trusted Architecture for Securely Shared Services 8

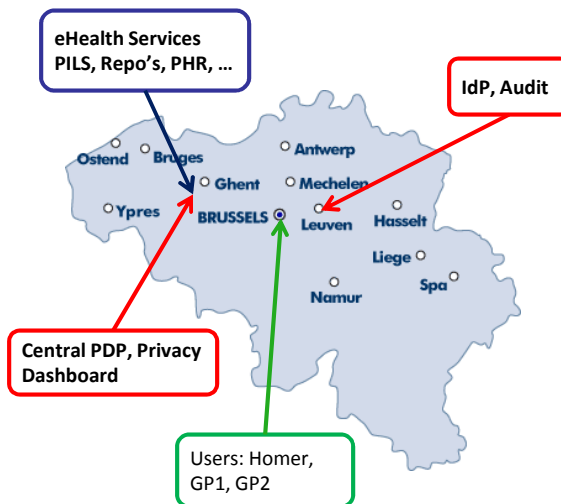
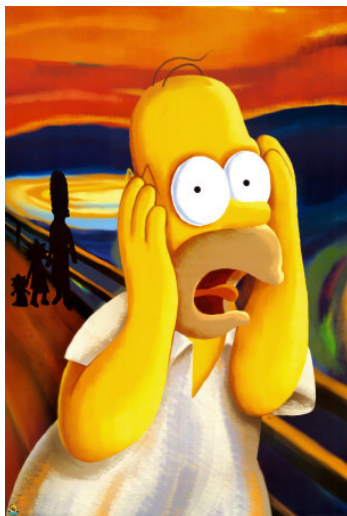


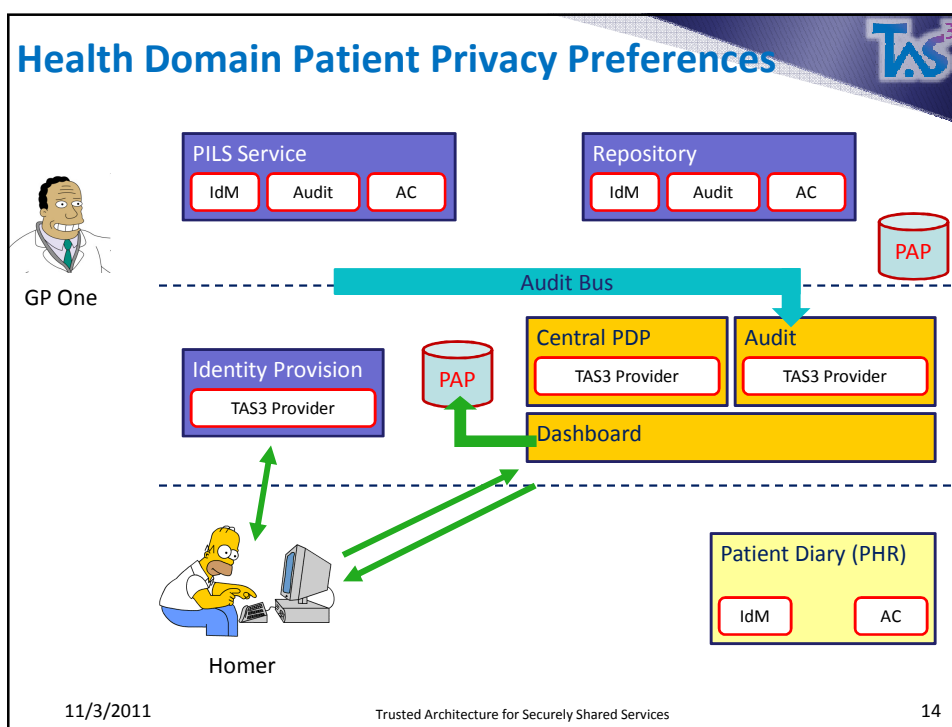
Dynamic Consent (Not demonstrated)

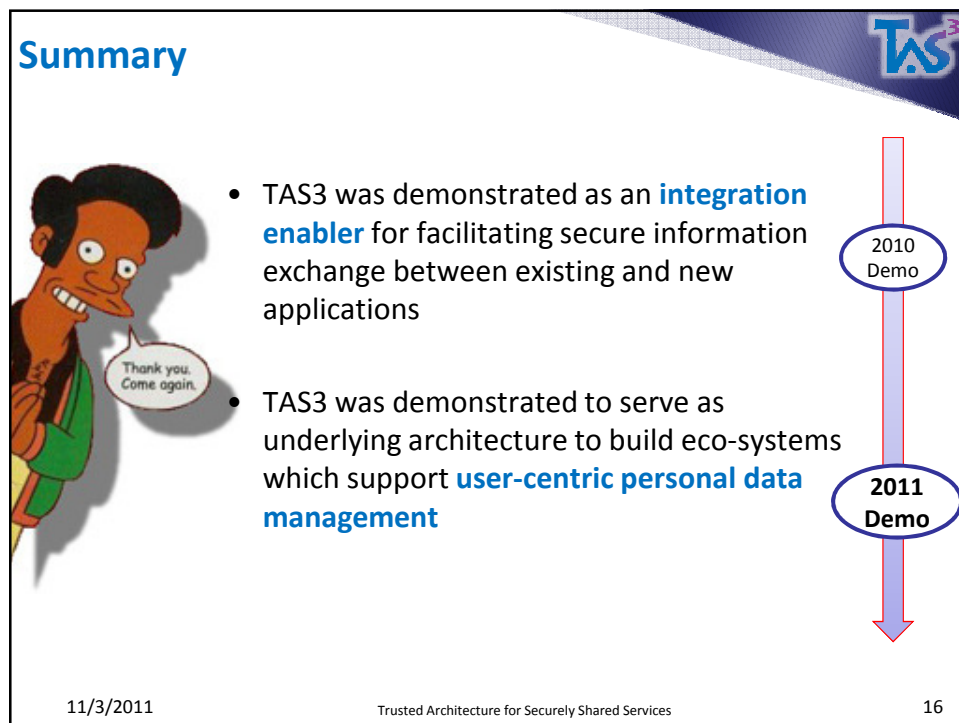
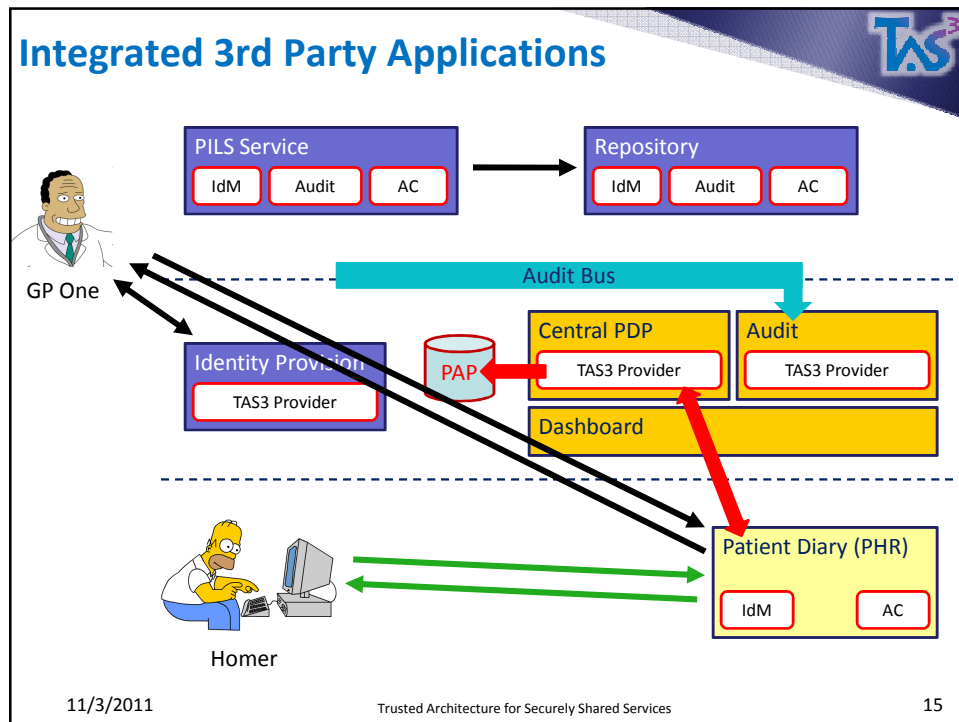
- Static & Dynamic expression of privacy preferences
 - Static Consent: previous scenarios are examples of “static”/”a-priori” privacy preferences
 - Dynamic Consent
- Scenario where the two are complementary
 - Static: consent to have medical information scanned for trial eligibility
 - Dynamic: A specific request for inclusion into a trial



Demonstration







Backup Slides



TAS3 Communication Stack (SSO, SLO, ID-FF DI, inter-SP communication)

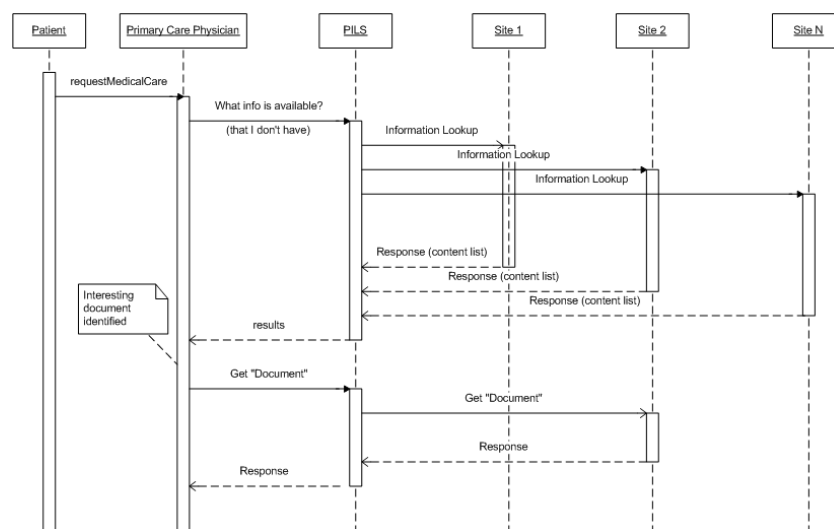
11/3/2011

Trusted Architecture for Securely Shared Services

17

Basic "Information Retrieval"

Backup Slide



11/3/2011

Trusted Architecture for Securely Shared Services

18

