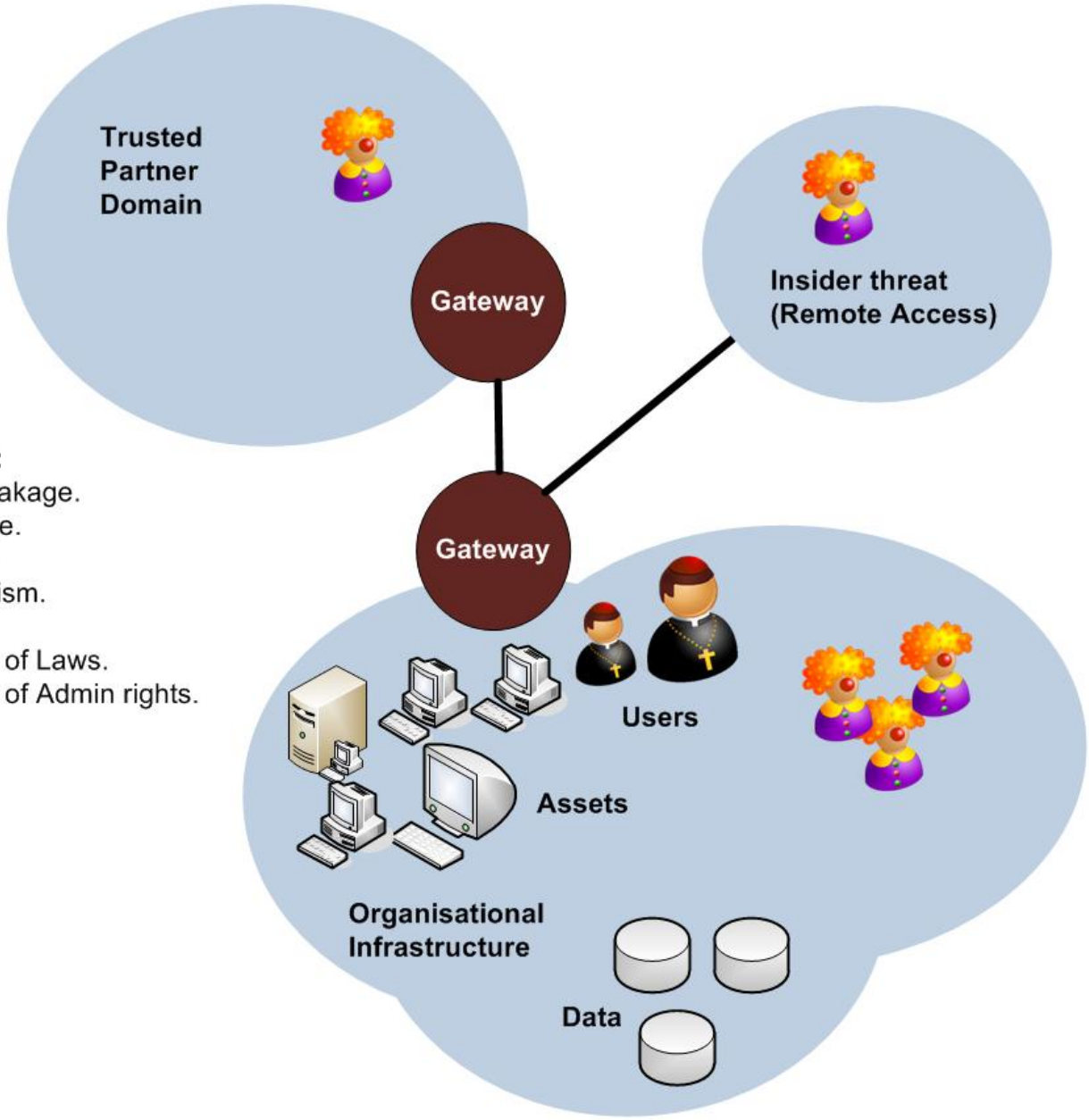
Next Generation Secure e-Health Platform

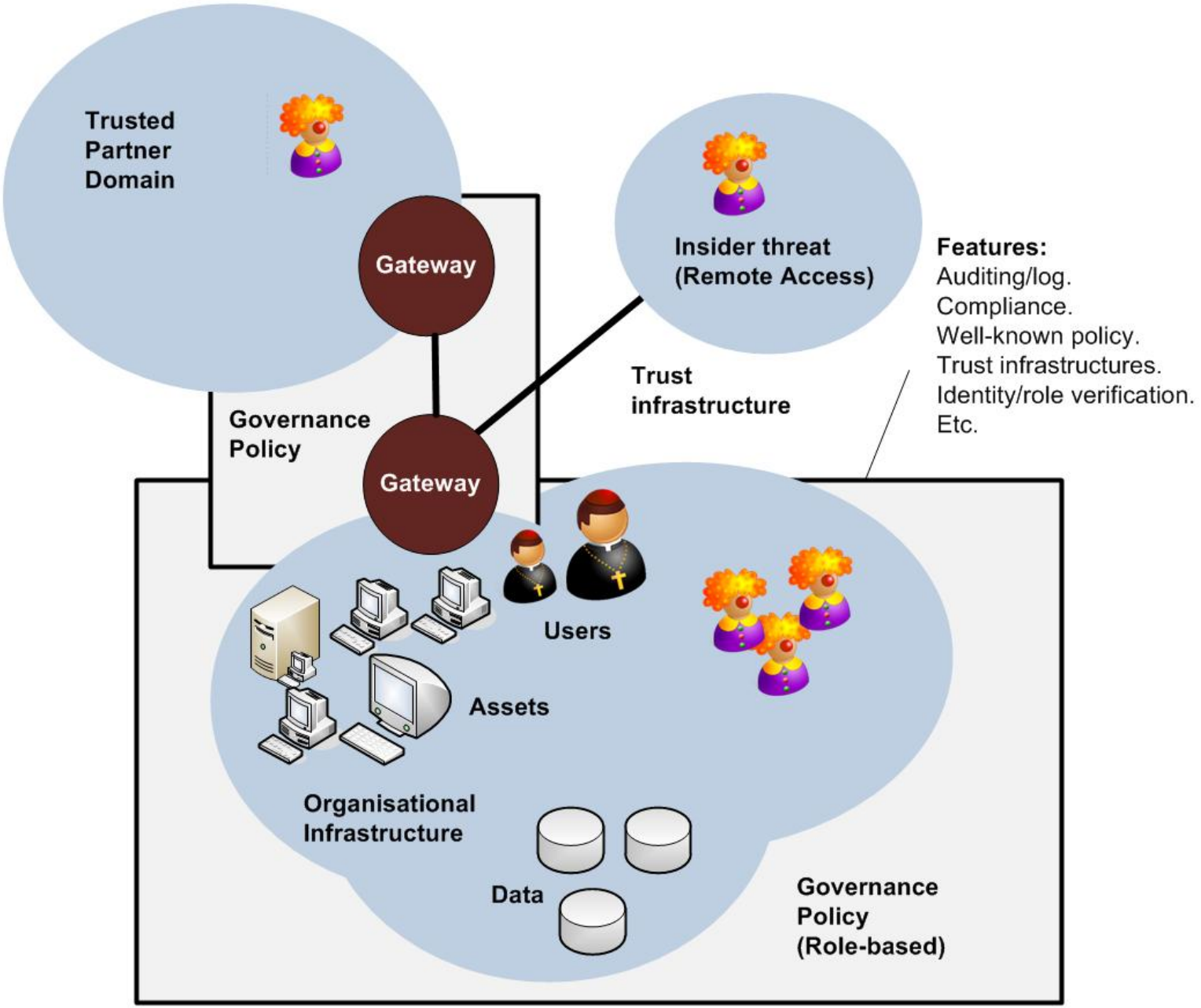
- Overview of information sharing.
- SPoC (Single Point of Contact) Principle.
- Information Sharing Context.
- E-Health Platform

Prof Bill Buchanan

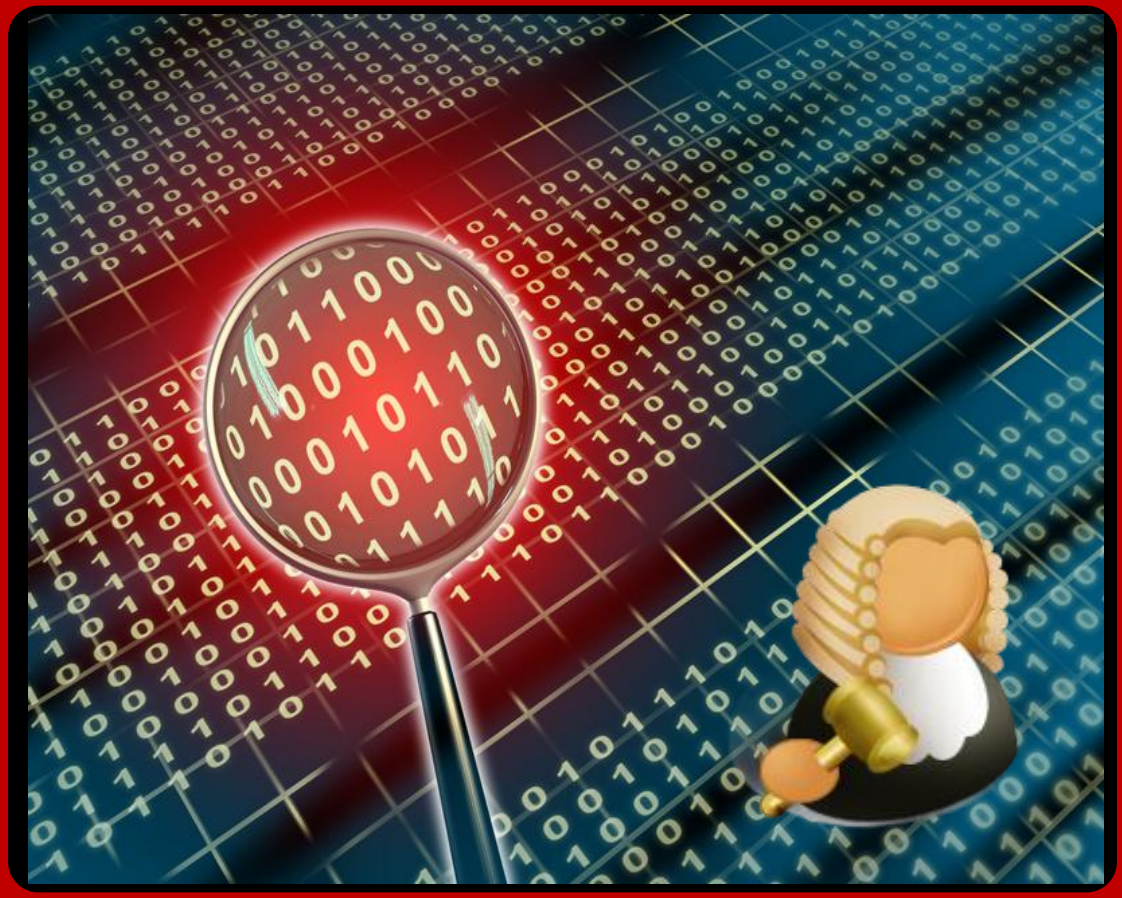
Author: Prof Bill Buchanan



Threat:
Data leakage.
Damage.
Abuse.
Vandalism.
Fraud.
Breach of Laws.
Breach of Admin rights.
Etc.


Trusted
Partner
Domain
Gateway
Insider threat
(Remote Access)
Features:
Auditing/log.
Compliance.
Well-known policy.
Trust infrastructures.
Identity/role verification.
Etc.
Trust
infrastructure
Governance
Policy
Gateway
Users
Assets
Organisational
Infrastructure
Data
Governance
Policy
(Role-based)

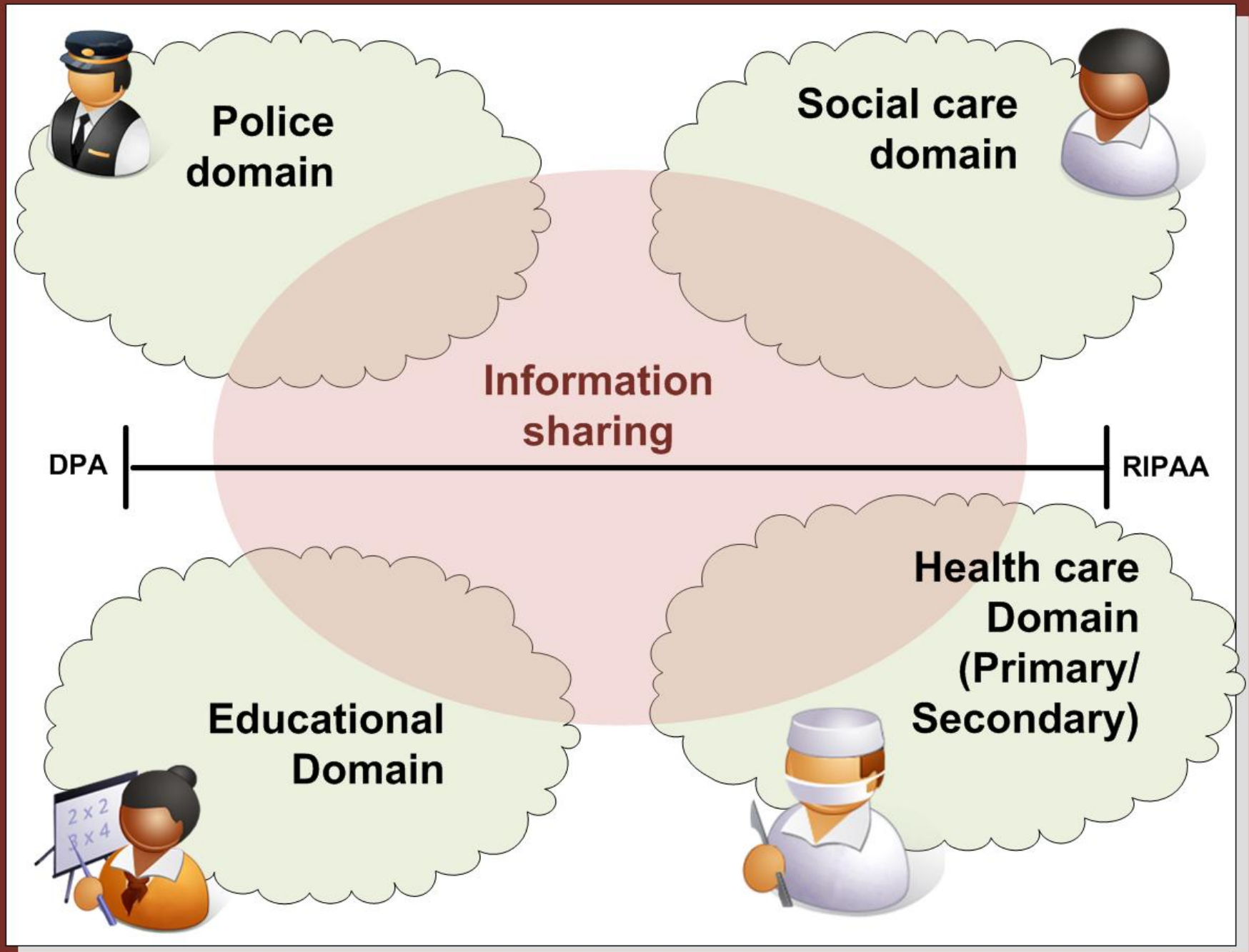
Information Sharing



centre for distributed computing & security

Context

Author: Prof Bill Buchanan



Sharing between domains

Police domain

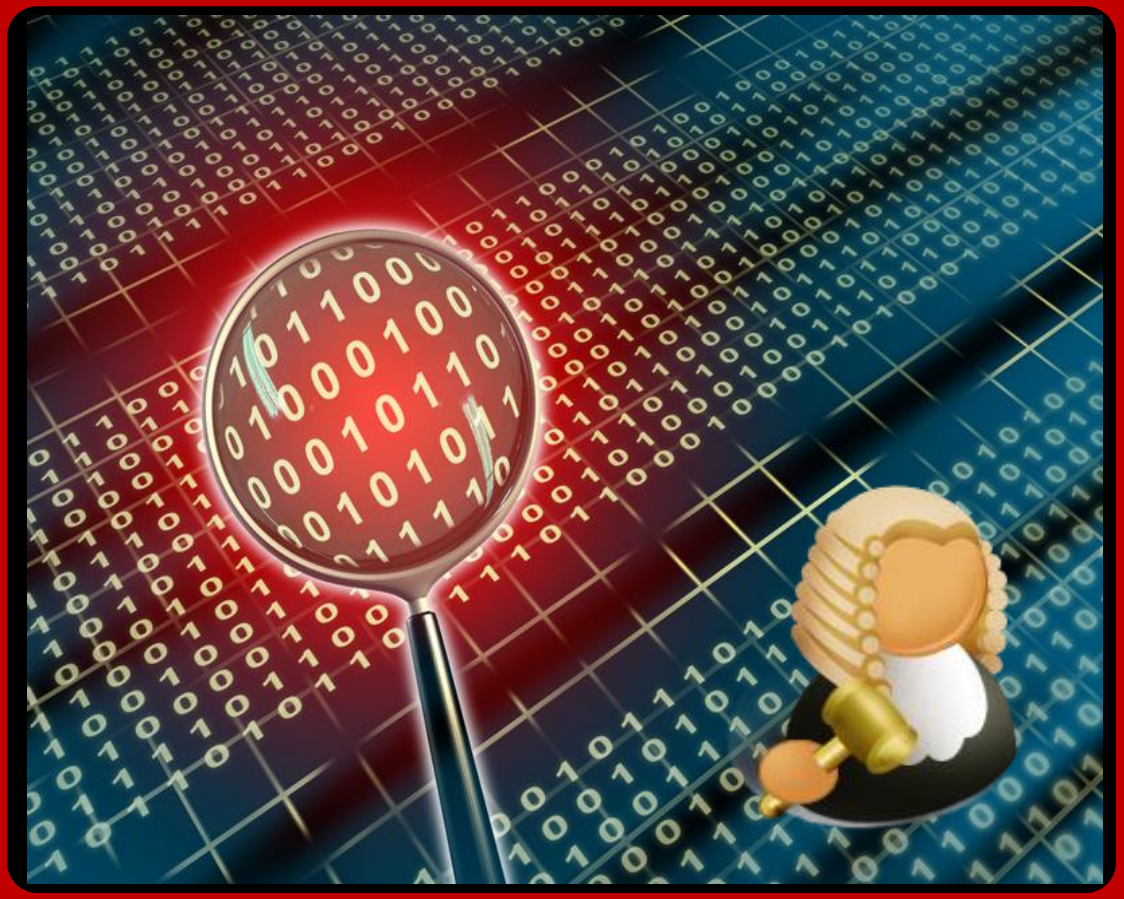
ILP (Intelligence-led policing) – proactive, researched and planned approach to policing and relies on a robust information-sharing mechanism.

MOPI (Management of Police Information)– best practices for consistent information recording, management and sharing

NIM (National Intelligence Model) – principles for communities to achieve common strategic, tactical solutions to common problems

Author: Prof Bill Buchanan

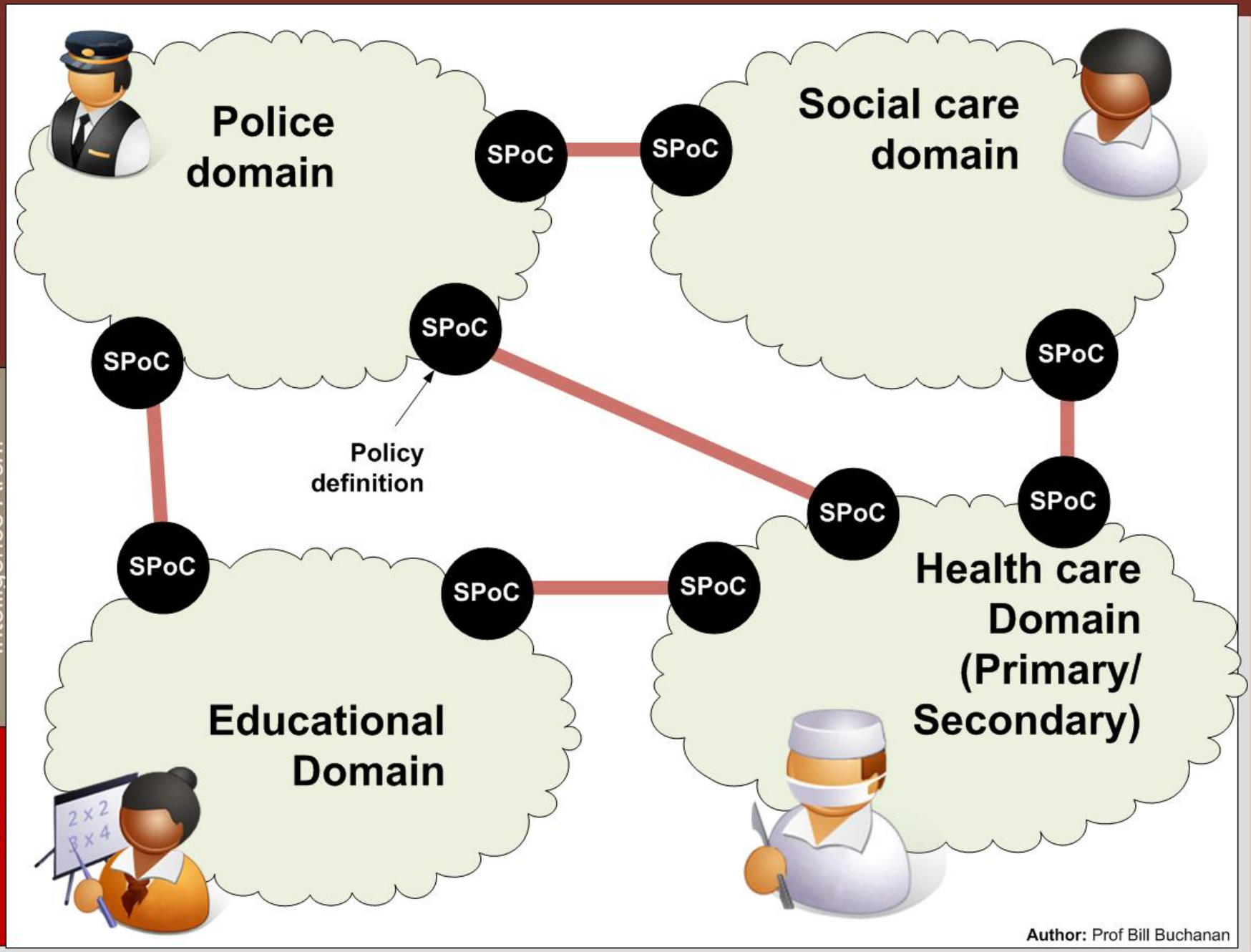
Information Sharing



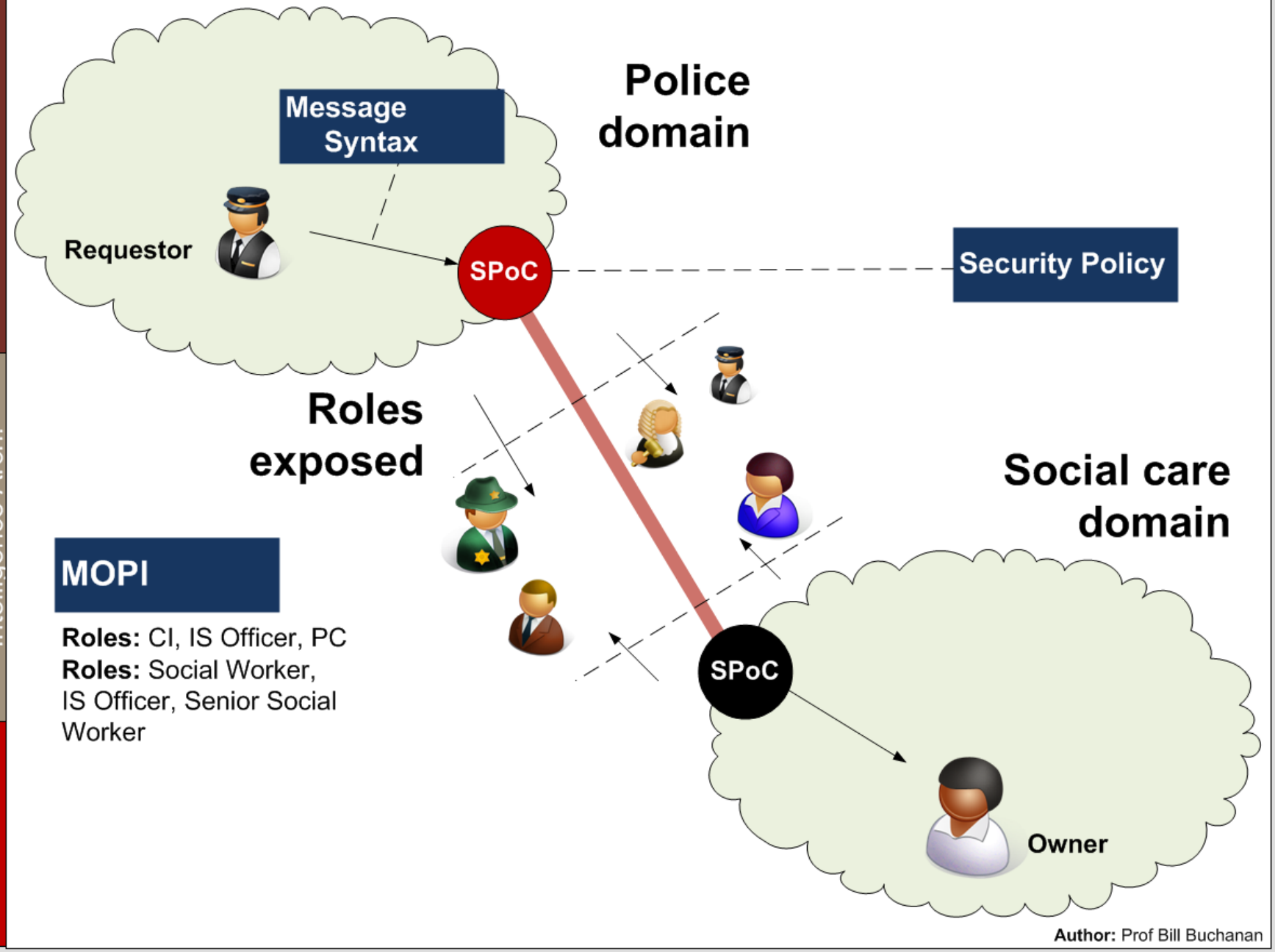
centre for distributed computing & security

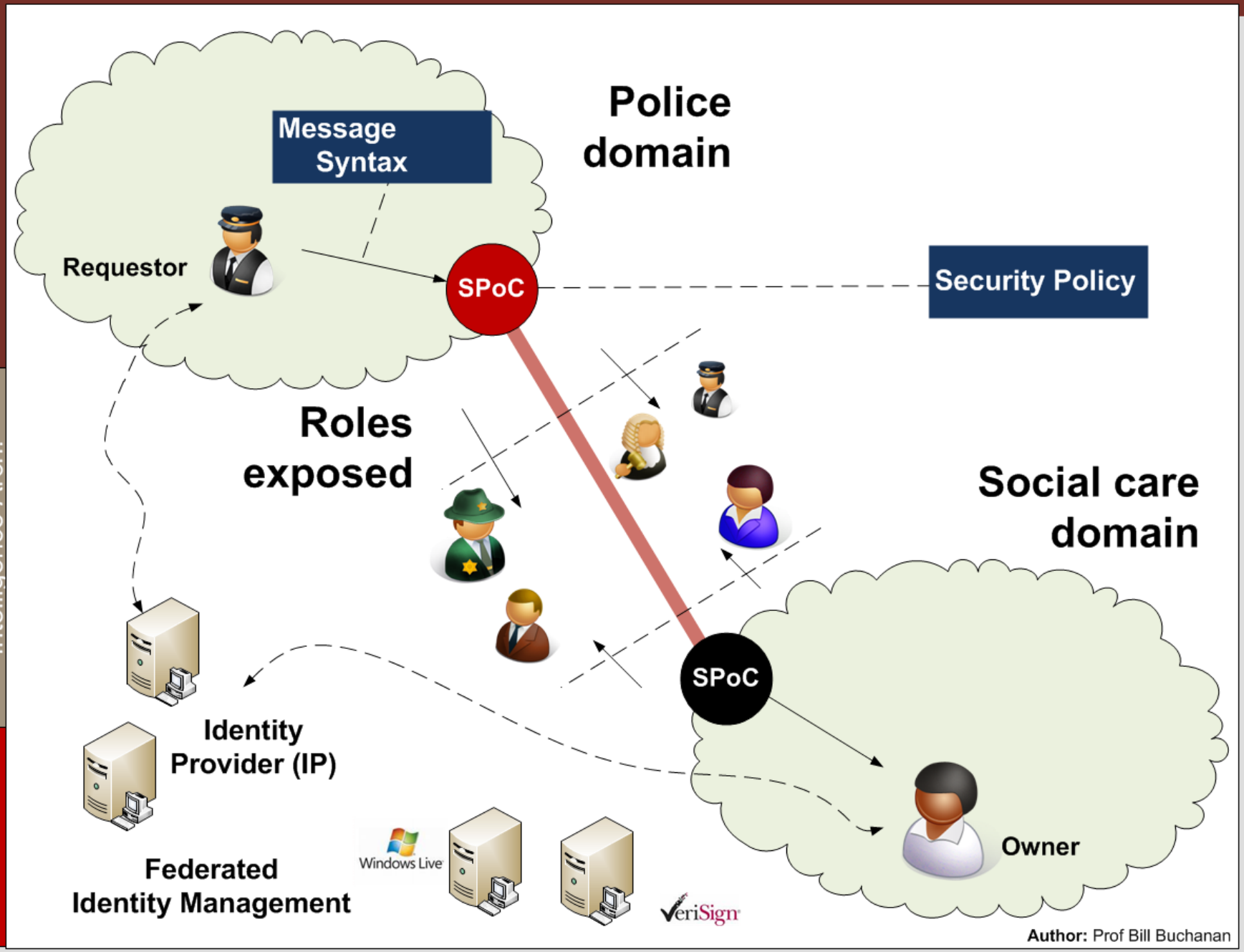
Information Sharing Architecture

Author: Prof Bill Buchanan

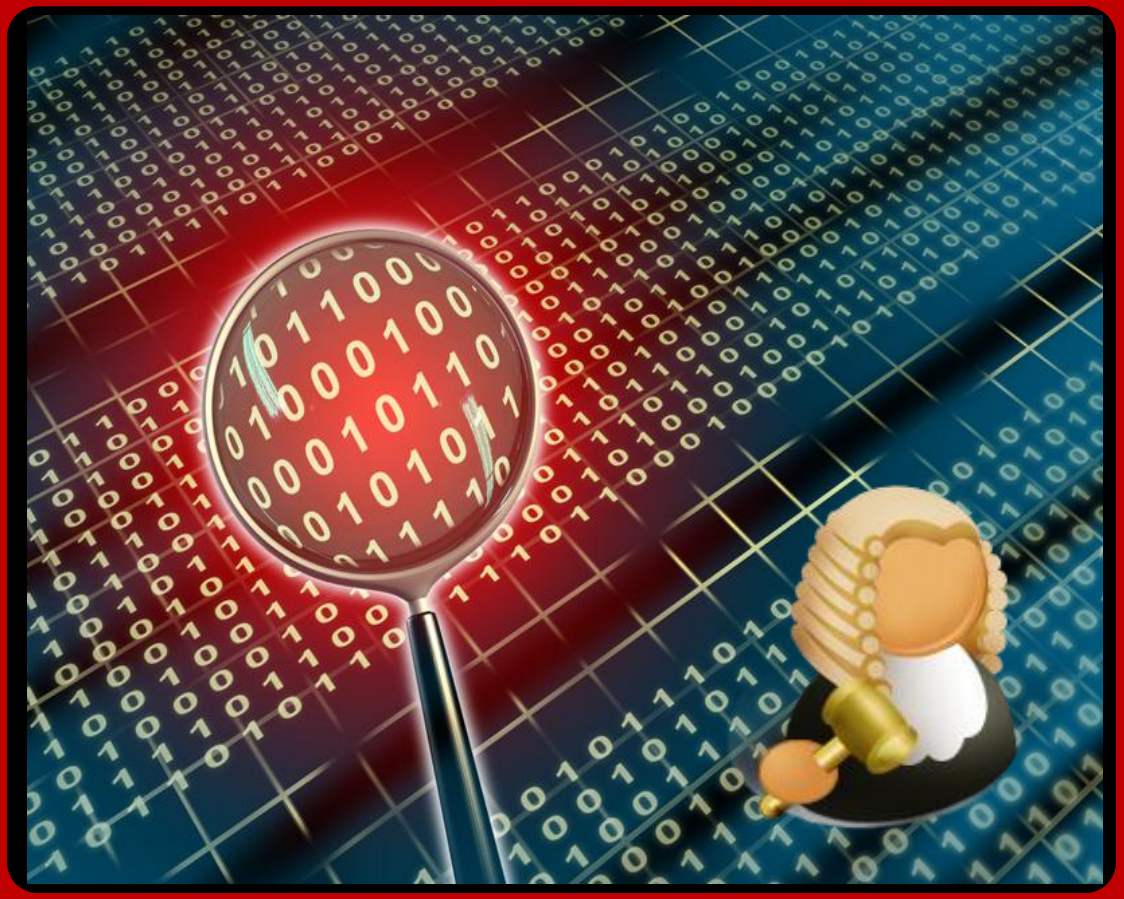


SPoC – Single Point of Contact


Police domain
Message Syntax
Requestor
SPoC
Security Policy
Roles exposed
Social care domain
MOPI
Roles: CI, IS Officer, PC
Roles: Social Worker, IS Officer, Senior Social Worker
SPoC
Owner
Author: Prof Bill Buchanan


Police domain
Message Syntax
Requestor
SPoC
Security Policy
Roles exposed
Social care domain
SPoC
Identity Provider (IP)
Owner
Federated Identity Management
Windows Live
VeriSign
Author: Prof Bill Buchanan

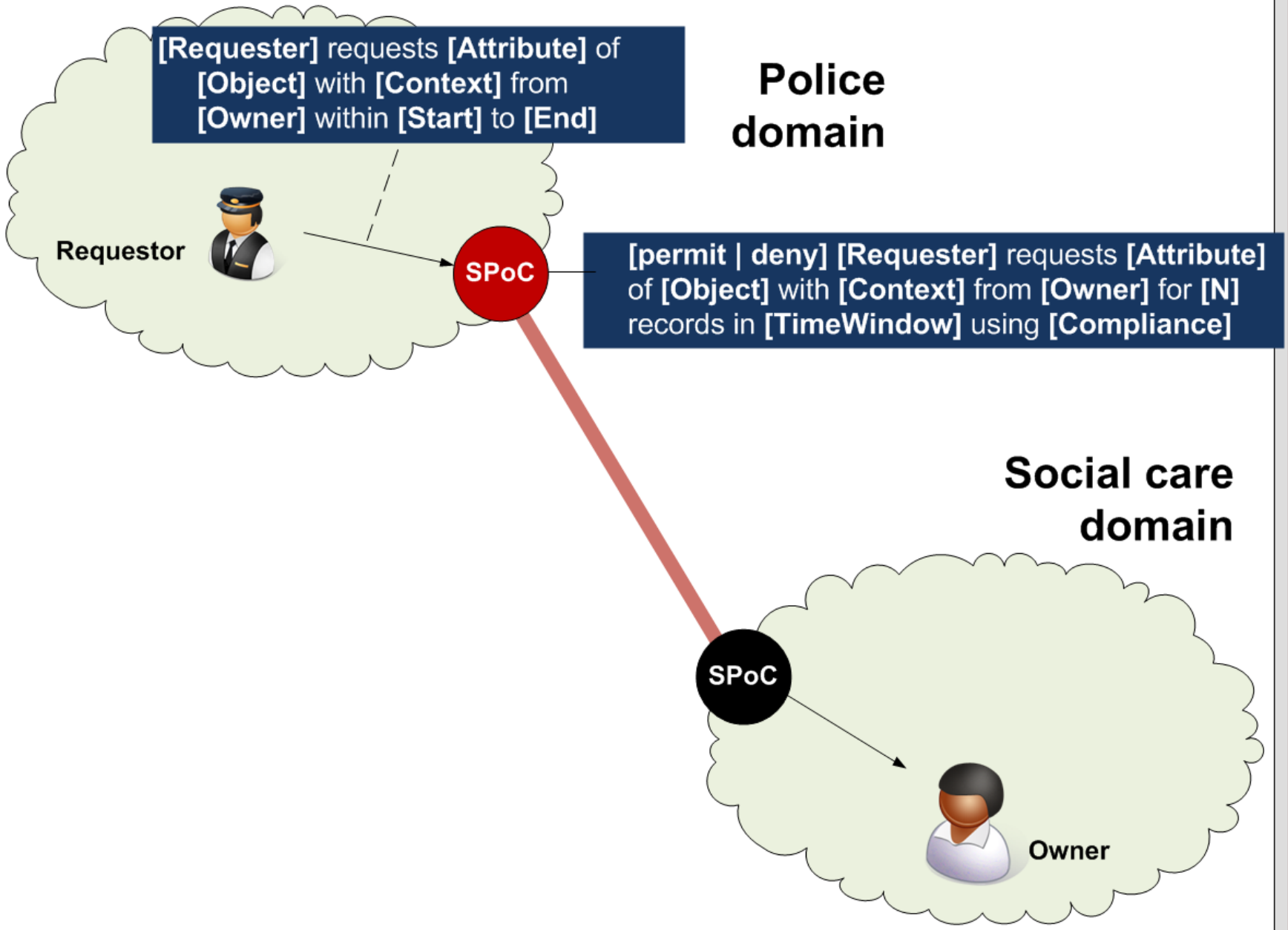
Information Sharing



centre for distributed computing & security

Message/Policy Syntax

Author: Prof Bill Buchanan


[Requester] requests [Attribute] of [Object] with [Context] from [Owner] within [Start] to [End]
Police domain
Requestor
SPoC
[permit | deny] [Requester] requests [Attribute] of [Object] with [Context] from [Owner] for [N] records in [TimeWindow] using [Compliance]
Social care domain
SPoC
Owner
Author: Prof Bill Buchanan

[Requester] requests **[Attribute]** of **[Object]** with **[Context]** from **[Owner]** within **[Start]** to **[End]**

Police domain

Requestor

SPoC

[permit | deny] [Requester] requests **[Attribute]** of **[Object]** with **[Context]** from **[Owner]** for **[N]** records in **[TimeWindow]** using **[Compliance]**

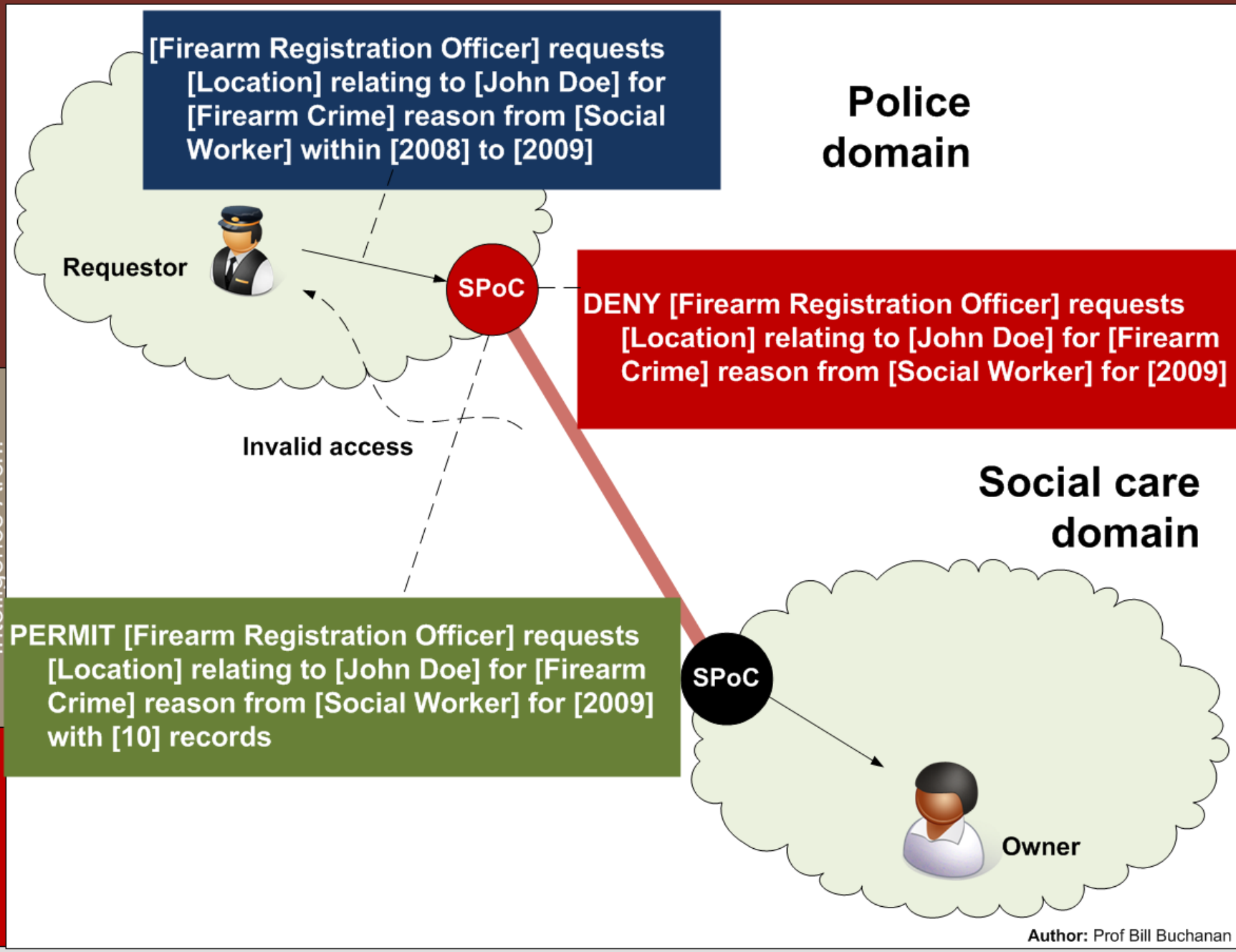
- **REQUESTER** = {Social worker, Doctor, Police Inspector…}.
- **ATTRIBUTE** = {Location, Identity, History, Behaviour, Interaction, Association}.
- **OBJECT** = Any searchable entity about which information is held and which is mapped to a UID within the domain.
- **CONTEXT** = {Crisis, Terrorism, Murder, Missing Person, Child/Adult Protection, Drugs, Volume Crime, Petty Crime, General Request}.
- **OWNER** = {Business Unit 1, Business Unit 2, …}.
- **TIMERANGE**= Definition of time.
- **RECORDS**= {n}.

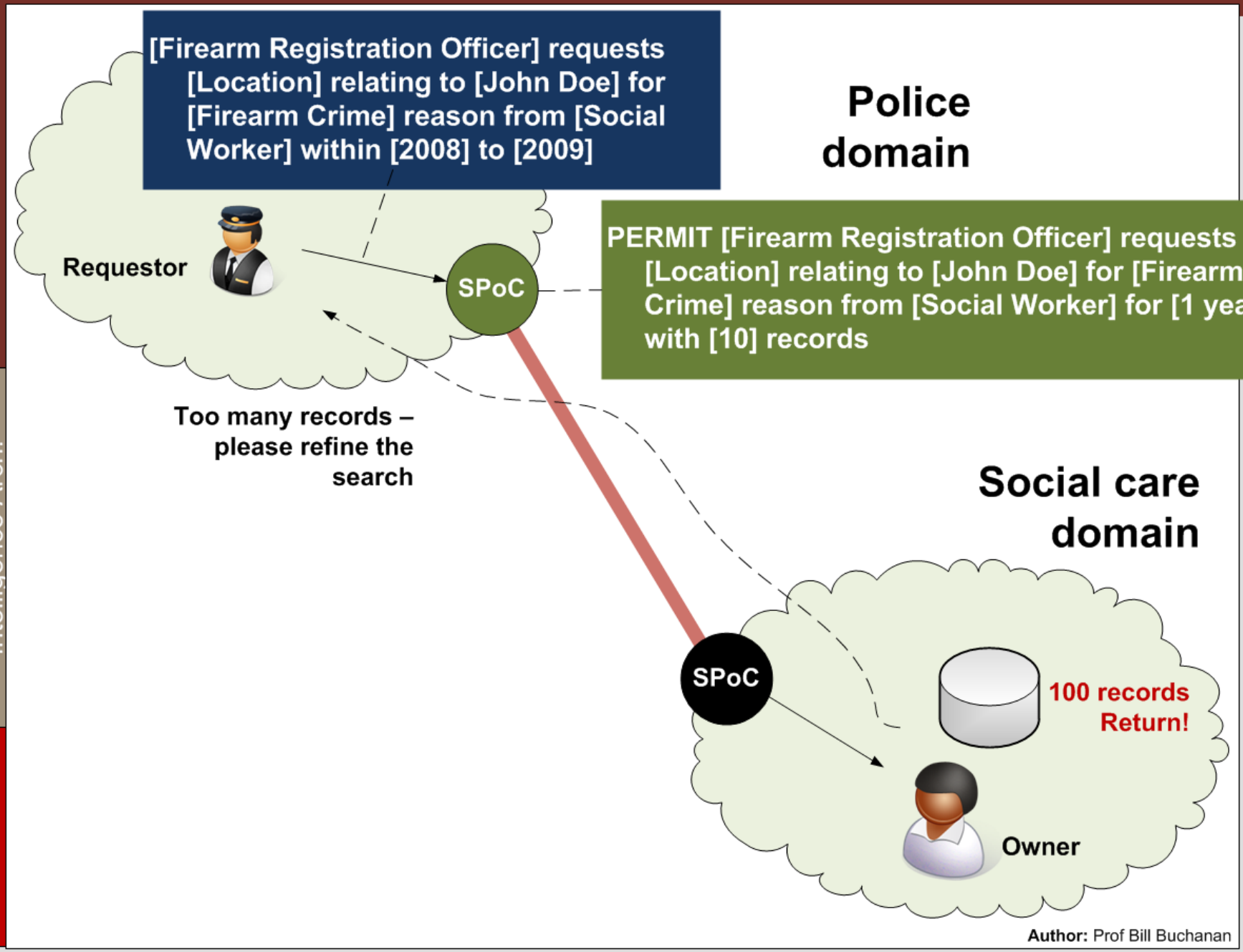
Social care domain

SPoC

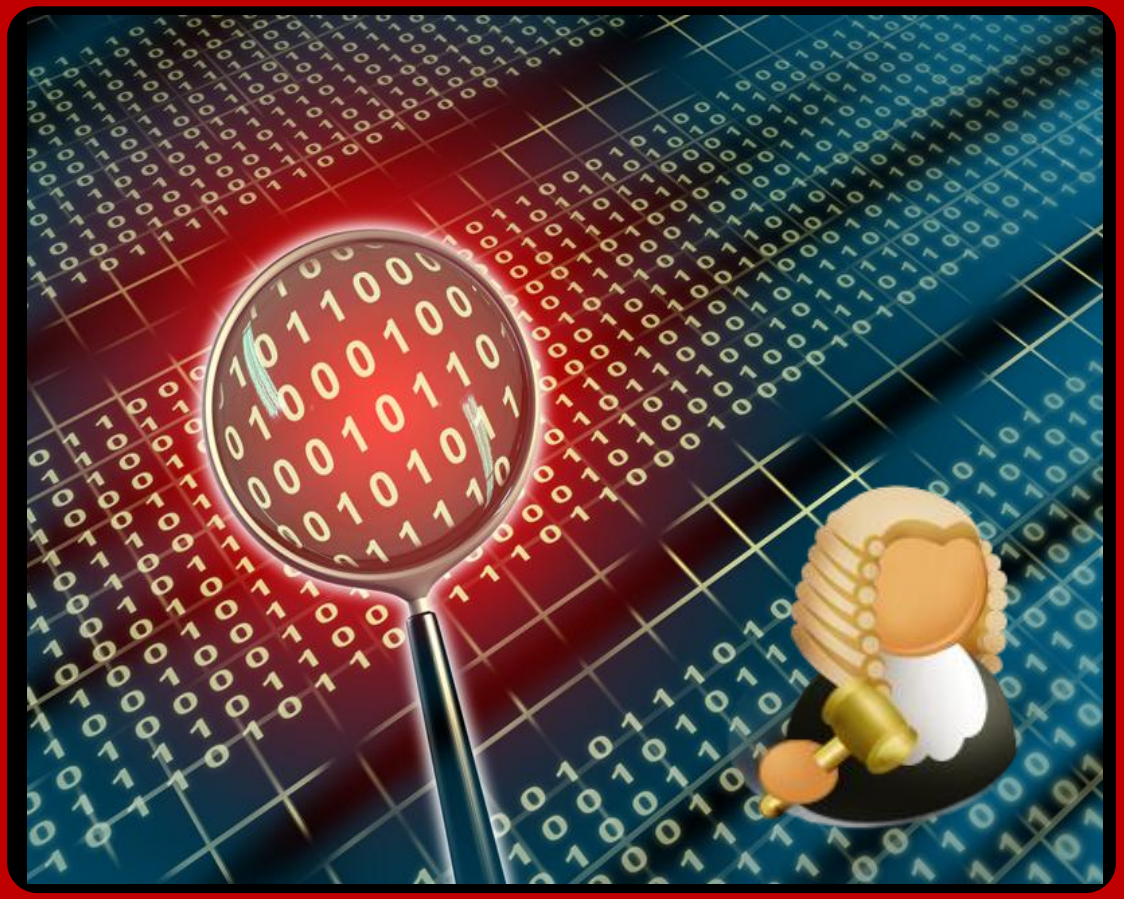
Owner

Author: Prof Bill Buchanan


[Firearm Registration Officer] requests [Location] relating to [John Doe] for [Firearm Crime] reason from [Social Worker] within [2008] to [2009]
Police domain
Requestor
SPoC
DENY [Firearm Registration Officer] requests [Location] relating to [John Doe] for [Firearm Crime] reason from [Social Worker] for [2009]
Invalid access
Social care domain
PERMIT [Firearm Registration Officer] requests [Location] relating to [John Doe] for [Firearm Crime] reason from [Social Worker] for [2009] with [10] records
SPoC
Owner
Author: Prof Bill Buchanan


[Firearm Registration Officer] requests [Location] relating to [John Doe] for [Firearm Crime] reason from [Social Worker] within [2008] to [2009]
Police domain
Requestor
SPoC
PERMIT [Firearm Registration Officer] requests [Location] relating to [John Doe] for [Firearm Crime] reason from [Social Worker] for [1 year] with [10] records
Too many records – please refine the search
Social care domain
SPoC
100 records Return!
Owner
Author: Prof Bill Buchanan

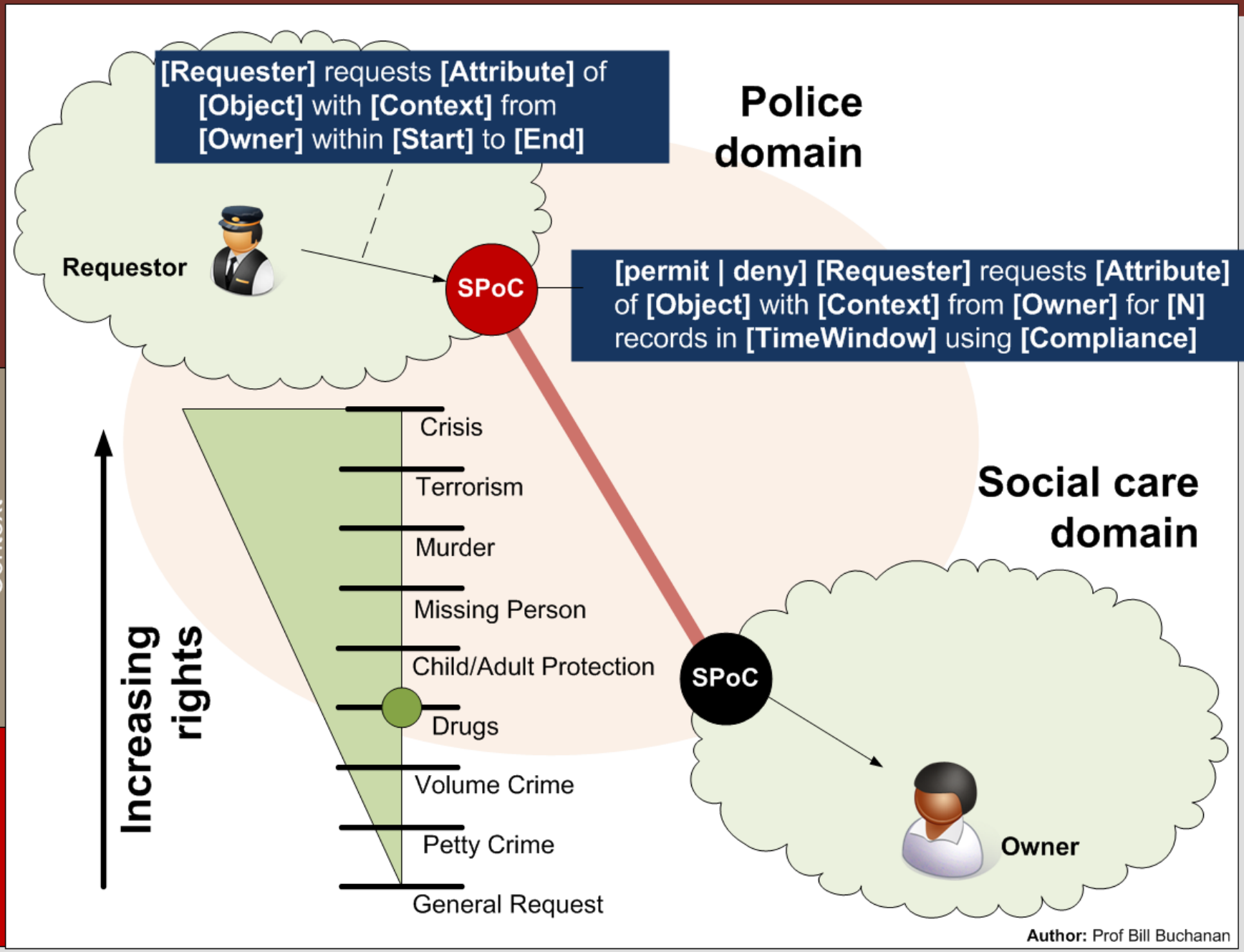
Information Sharing

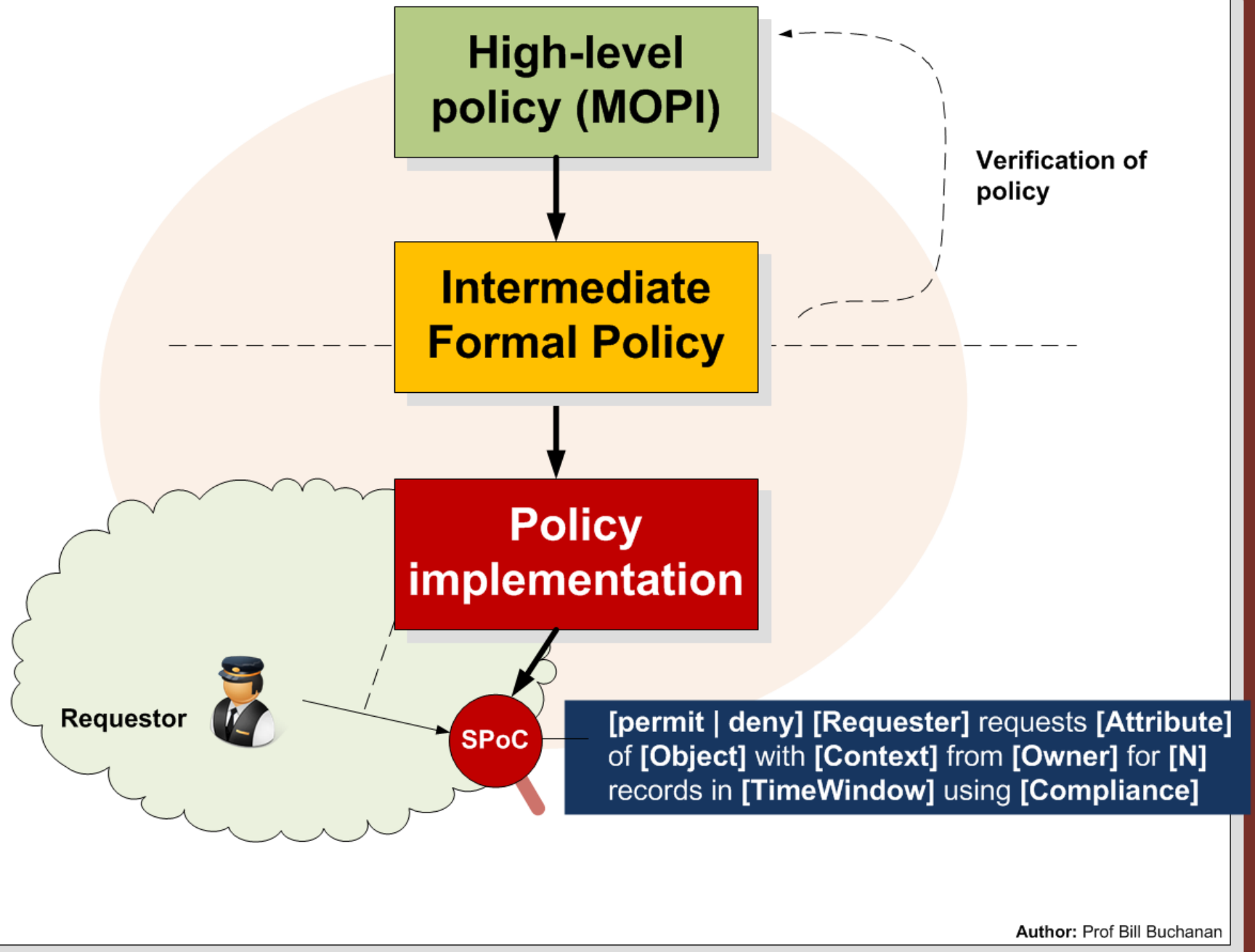


centre for distributed computing & security

Context

Author: Prof Bill Buchanan


[Requester] requests [Attribute] of [Object] with [Context] from [Owner] within [Start] to [End]
Police domain
Requestor
SPoC
[permit | deny] [Requester] requests [Attribute] of [Object] with [Context] from [Owner] for [N] records in [TimeWindow] using [Compliance]
Crisis
Terrorism
Murder
Missing Person
Child/Adult Protection
Drugs
Volume Crime
Petty Crime
General Request
Increasing rights
Social care domain
SPoC
Owner
Author: Prof Bill Buchanan


High-level policy (MOPI)
Verification of policy
Intermediate Formal Policy
Policy implementation
Context
BCS
Requestor
SPoC
[permit | deny] [Requester] requests [Attribute] of [Object] with [Context] from [Owner] for [N] records in [TimeWindow] using [Compliance]
Author: Prof Bill Buchanan

Next-generation Information Sharing Infrastructure

- Scalable architecture.
- Enhanced security.
- No need to expose data structure to other domains.
- Well defined policies.
- Integrated auditing/compliance.
- Context allows access, if required.
- Lock-down (explicit deny).
- Interchange between any domain.
- Links to any domain.
- Customised policies between domains.

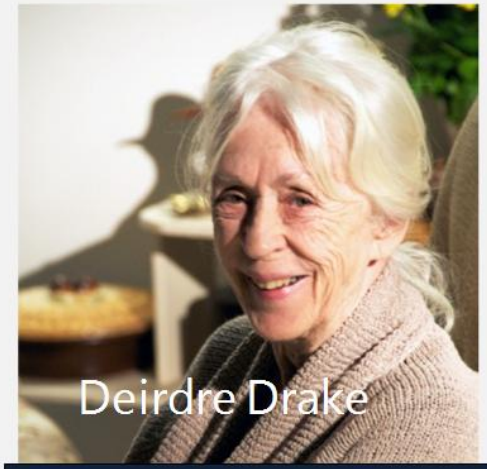
Author: Prof Bill Buchanan

A Next Generation Cloud-based Health Care Platform – Towards Trust and an Infinite Possiblities

Napier: Bill Buchanan, Christoph Thuemmler, Lu Fan, Elias Ekonomou, Owen Lo.
Imperial: Prof Derek Bell

- Healthcare Professional.
- Invited user

- Site Creator
- Primary Carer



- Care Subject
- 82 years old
- House bound
- COPD (Chronic Obstructive Pulmonary Disease)

- Invited user

PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab

DACAR e-Health Platform

Trusted Services

Chelsea and Westminster Hospital NHS
NHS Foundation Trust

Microsoft

Edinburgh Napier UNIVERSITY

Clinical Services

HoIP

kodit

Patient Simulator

Patient Cloud

Imperial College London

Edinburgh Napier UNIVERSITY

CIPHER LAB

Research Services

Patient Capture

GS1 UK

Technology Strategy Board
Driving Innovation

EPSRC
Pioneering research and skills

Societal

Technical

Lack of integration between assisted living, primary and secondary care

Patient records are often static

Aging population

Different systems/formatting used for data

Lack of information sharing across the public sector

Limited/difficult access methods … typically Government infrastructures … lack of trust

Strong demand to consume health care data

Poor access control to data

Lack of integration with careers and trusted people

Data often aggregated and context is often lost

Some key issues

PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab

Rights

Clinical Services

Digital Trust

Human Trust

Strong Governance

Identity

Infinite possiblities

Translation of rights
Translation of identities

Strong Governance
Policy

Assisted Living (Informal and Trust based)

Primary Health Care (Formal and role-oriented)

Secondary Health Care (Formal and role-oriented)

Manager might ask: What's difference in length-of-stay between different age categories for June?

Consultant might ask: How does the Early Warning Score affect the length-of-stay?

Family friend might ask: In which ward is Deirdre?

PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab

PatientID

Static Patient Record

- Often localised
- Different systems/formats
- Poor access control
- Poor identity verification
- Cannot be aggregated
- Etc.

Clinical Services

ConsumerID (RoleID)

Domain A

Data Storage (within the Cloud in buckets)

PatientID Bucket

Dynamic Patient Records

Security Policy (including interdomain rights)

CaptureTime

Capturer ID (RoleID)

PatientID

EventID

DeviceID

ClinicalMeasureID (ClinicalUnitsID)

LocationID

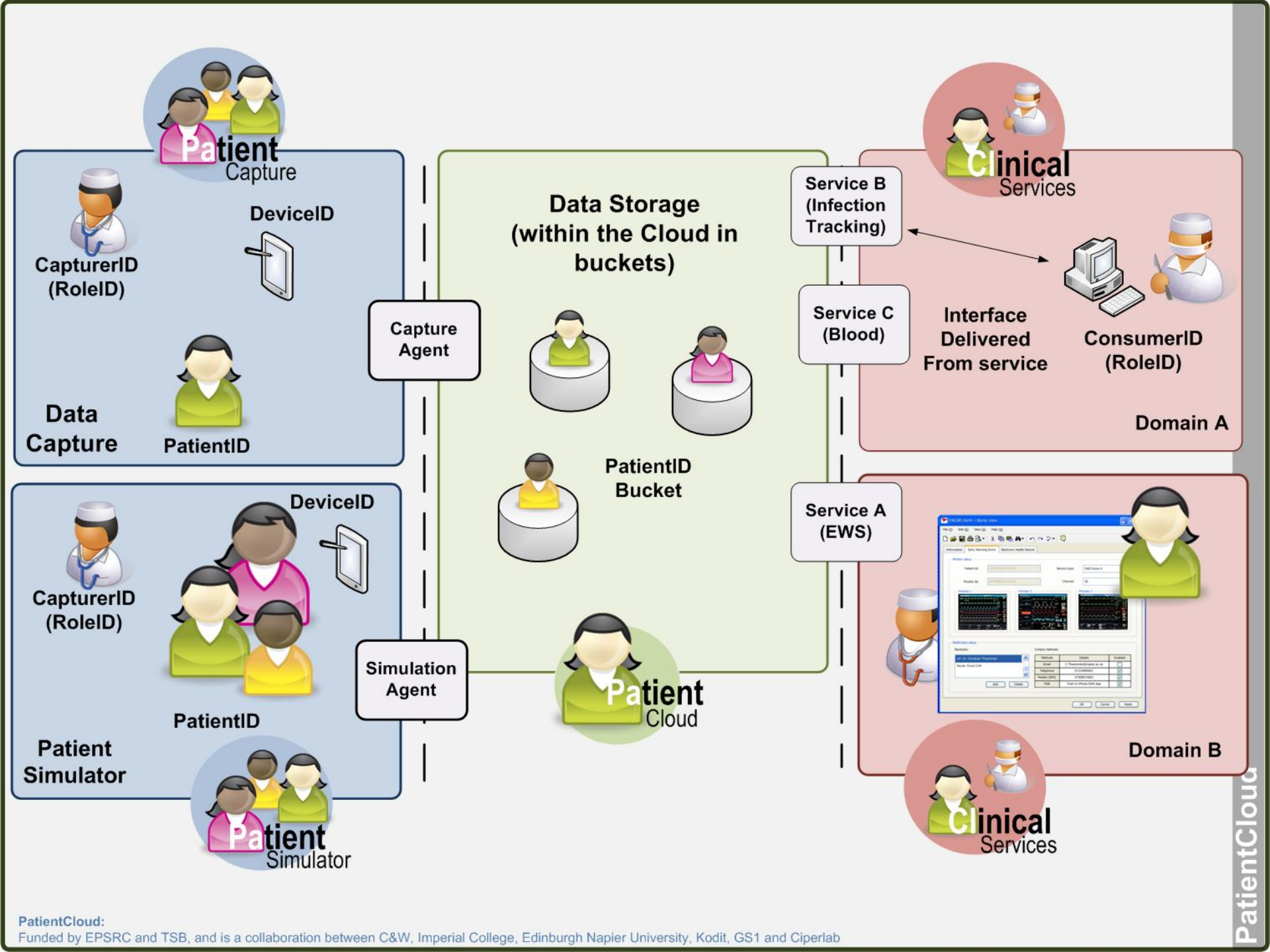
AreaID

Patient Capture

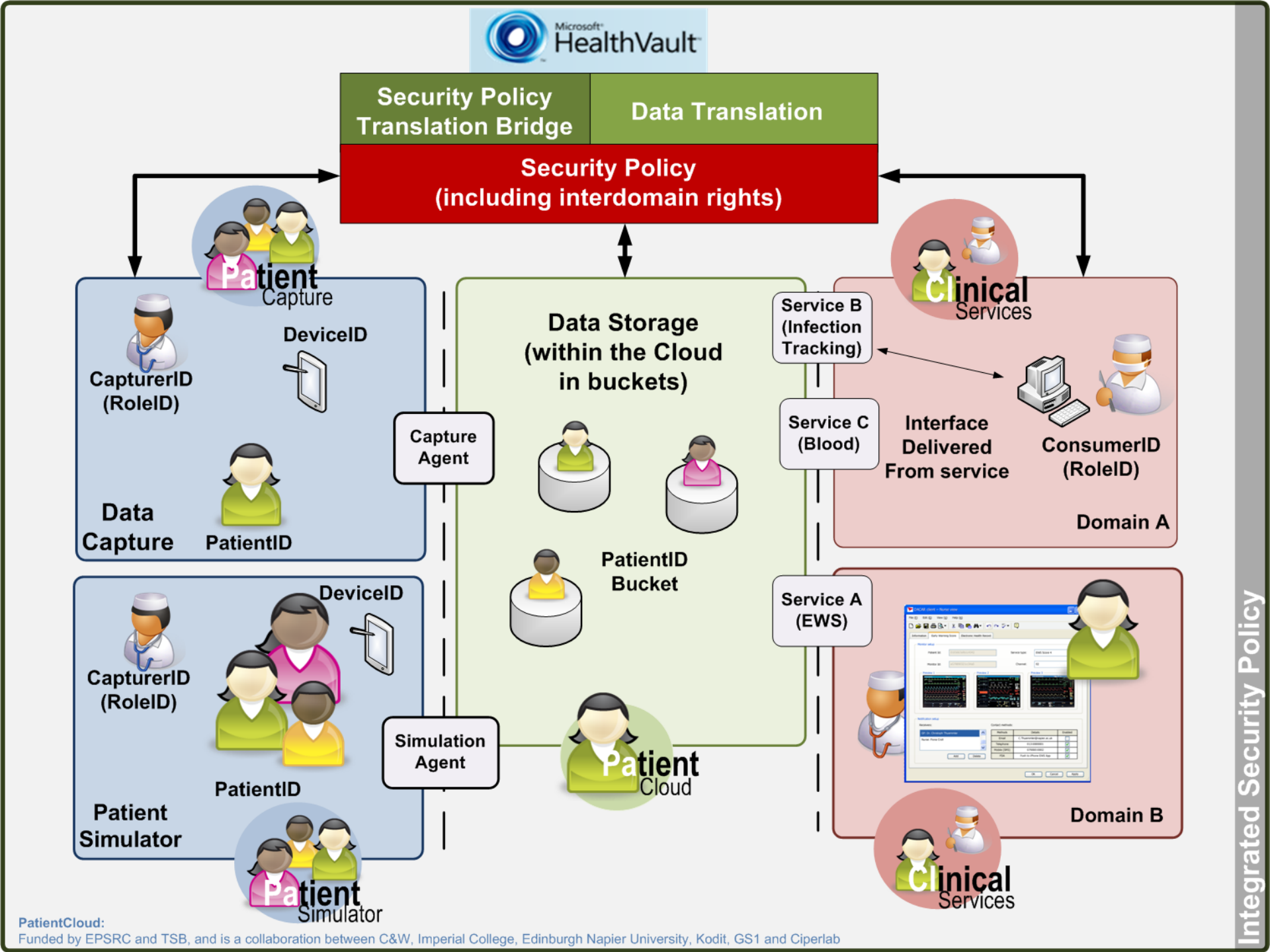
Patient Cloud

Why?

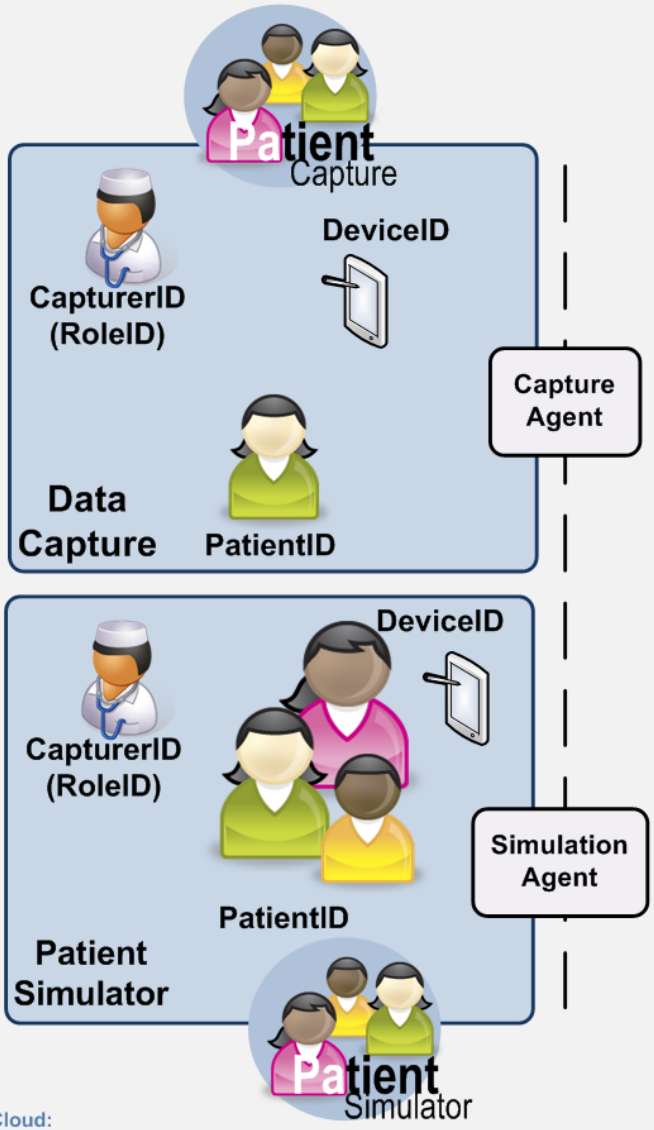
PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab

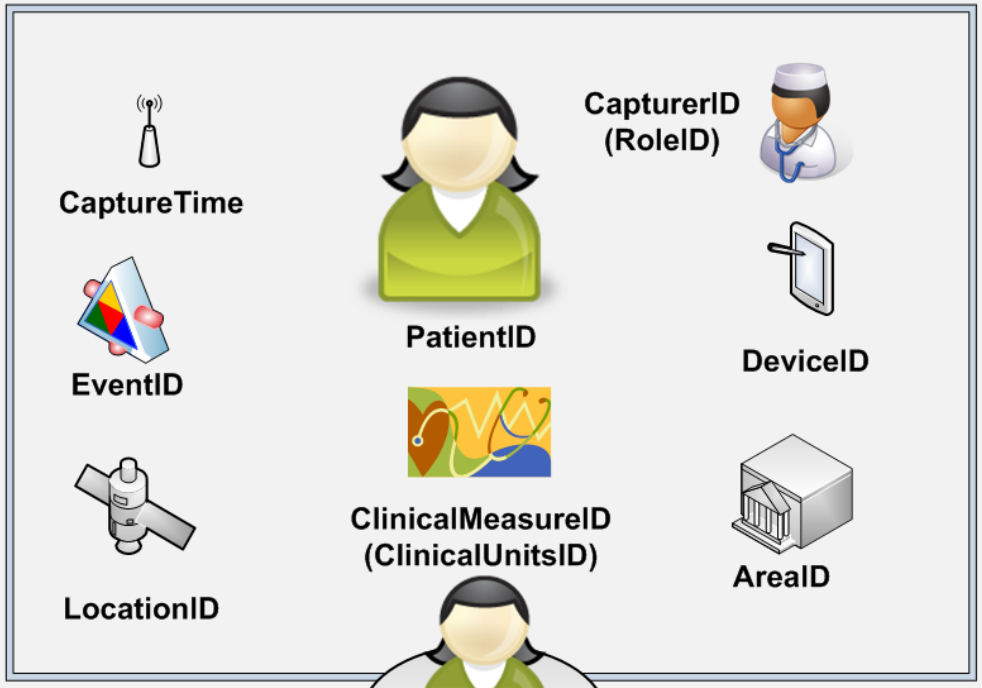


PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab

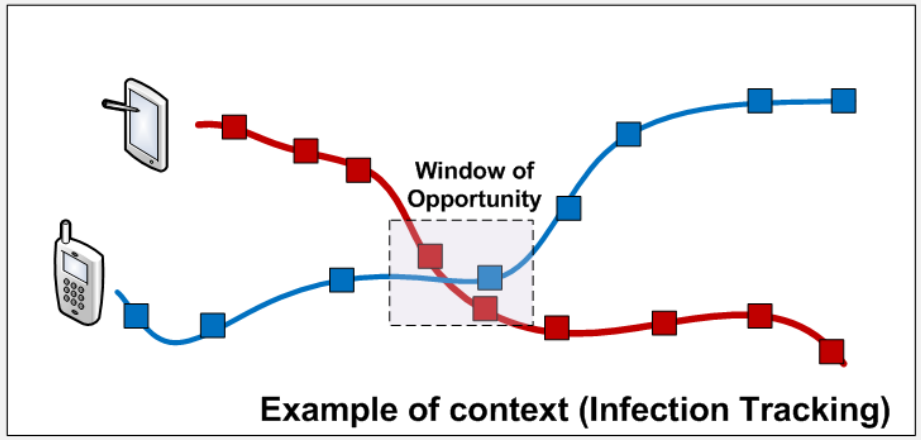


PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab

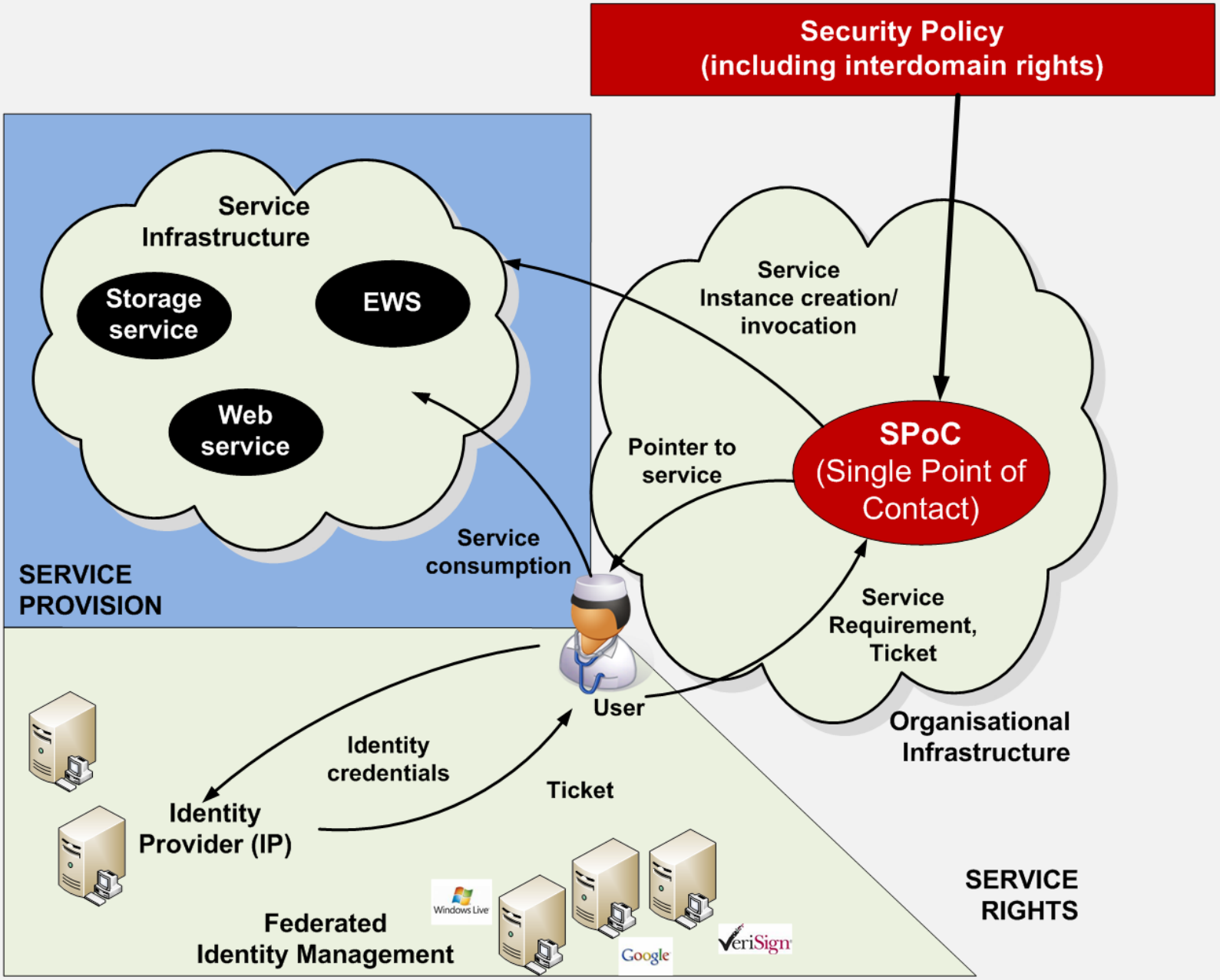




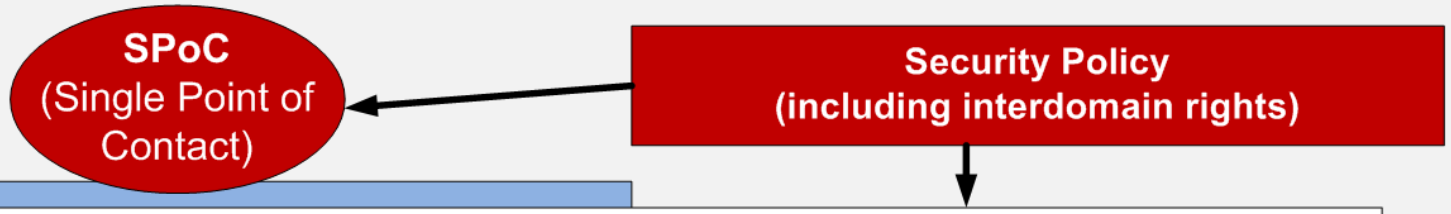
PatientID
Bucket



PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab



PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab



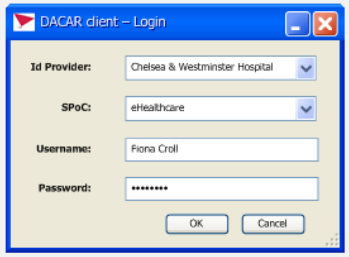

```
[permit] [Medical Staff] [C | R] [Temp | SpO2 | HR | BP | RR | Pain] of [Patient26078] with
[EWS] from [Chelsea & Westminster Hospital] for [*] records in [P2010-12-30T00:00:00] using
[Data Protection Act]

[permit | deny] [Requester] [C | R | U | D] [Attribute] of [Object] with [Context] from
[Owner] for [N] records in [Time Window] using [Compliance].
```

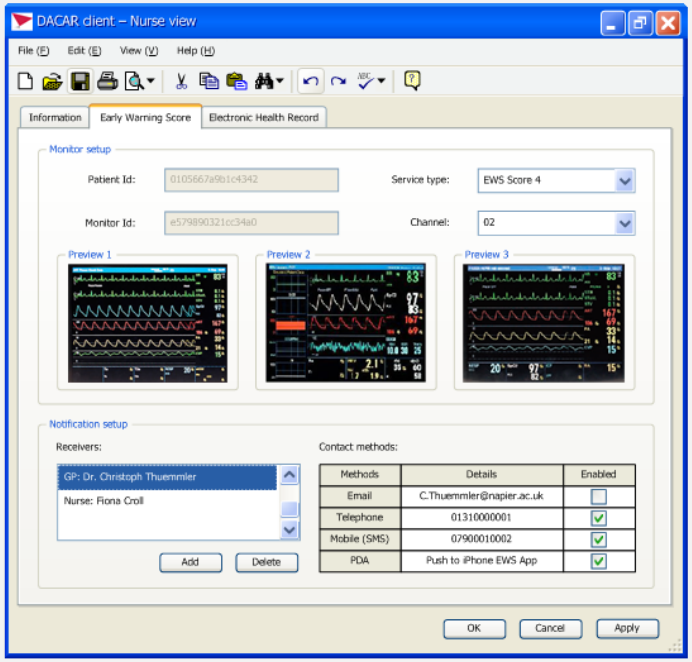
A similar syntax is also applied to the request messages:

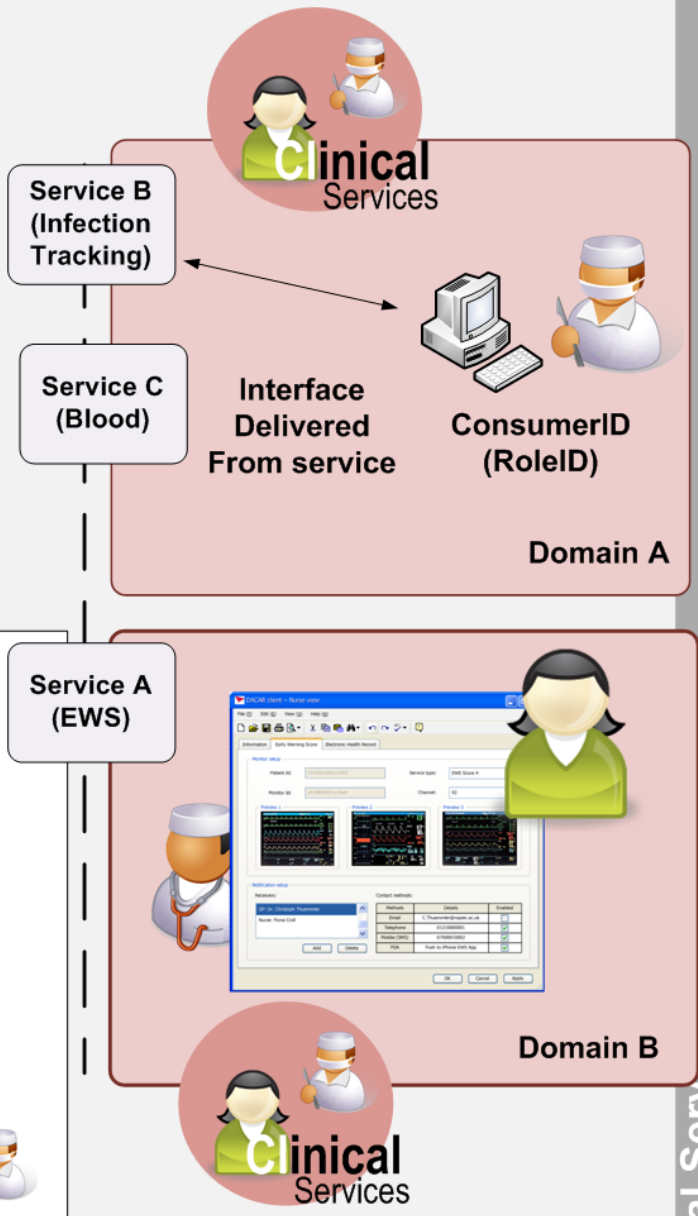
```
[Requester] [C | R | U | D] [Attribute] of [Object] with [Context] from [Owner] within
[Start] to [End]
```

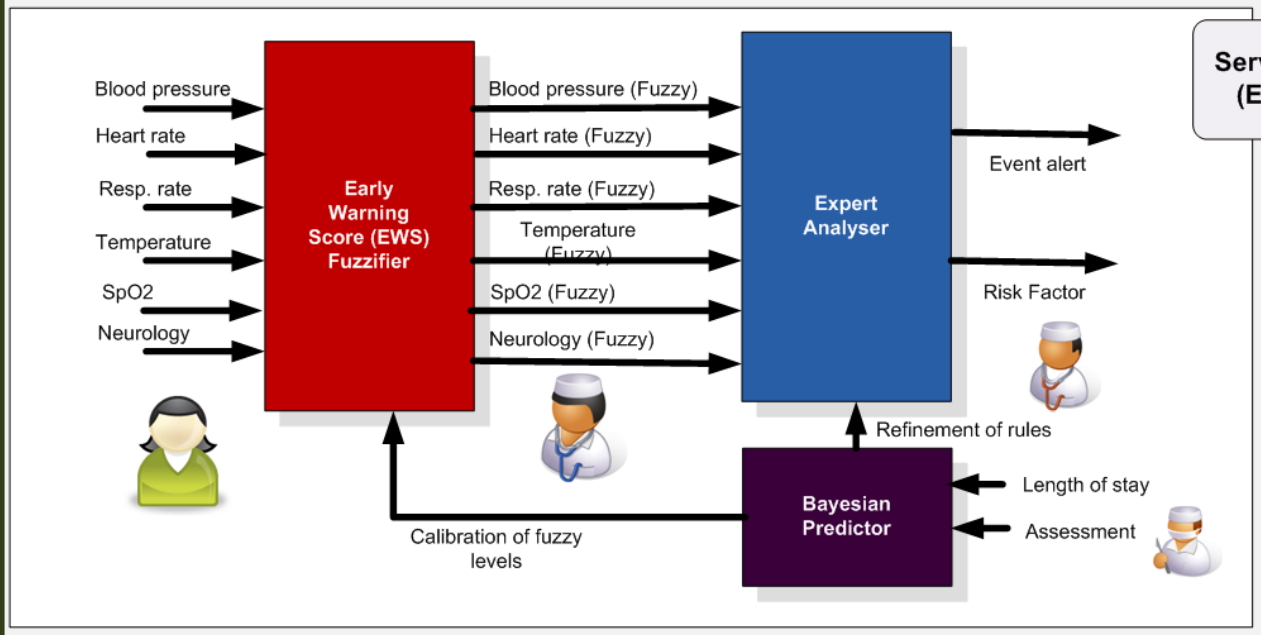
- { [permit | deny] This is part of the rule syntax which indicates the action of the rule. This defines whether a request meeting the rule criteria will be permitted or denied access.
- { [Requester] This identifies a request sender's role, e.g. GP, or pseudonym, e.g. 10420, or a combination of the two, e.g. GP10420.
- { [C | R | U | D] This defines detailed permissions for a requester to create, read, update and delete certain information.
- { [Attribute] This is a unit of information describing an object. An attribute may be a primitive data type, e.g. the pseudonym of an object as a string, or a complex data type, e.g. a person's ECG record for 45 seconds.
- { [Object] This is part of DACAR's system model. It refers to any entities in a healthcare scenario, about which information is held.
- { [Context] This identifies the reason why the information is being shared. The context governs the level of access and permissions associated with information exchange, and hence defines the priority accorded to information requests.
- { [Owner] This species a role with sufficient privileges to manage all aspects of an information source. The owner has the authority to allow or deny access to an information element, as required by legislation and defines responsibilities.
- { [N] records in [Time Window] This defines the number of records permitted over a period of time, where N can be any positive integer.
- { [Compliance] This refers to legislative requirements that support the exchange of information, such as the Data Protection Act, the Human Rights Act, the Freedom of Information Act and so on.
- { [Start] and [End] These identify the start and end of the date/time period over which information shown.

Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab









PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab

Patient Simulator

Clinical Services

Service B (Infection Tracking)

Service C (Blood)

Interface Delivered From service

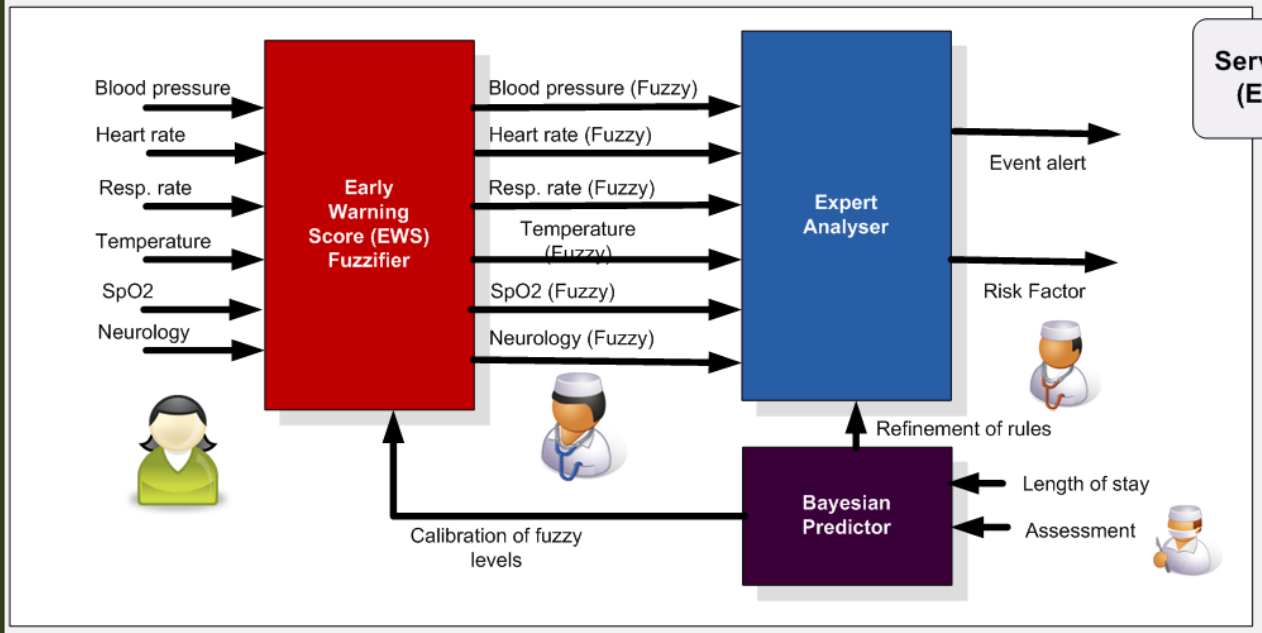
ConsumerID (RoleID)

Domain A

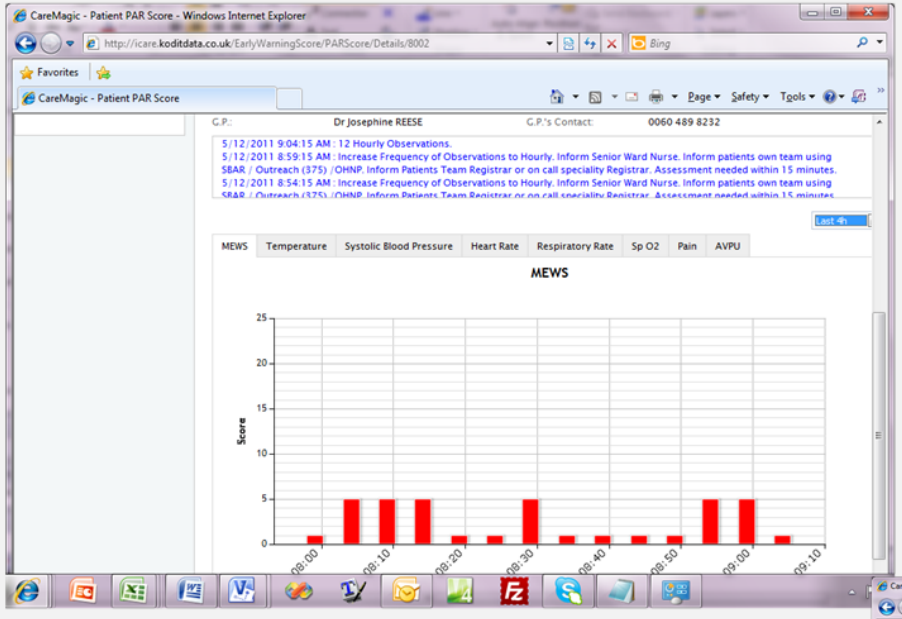
Service A (EWS)

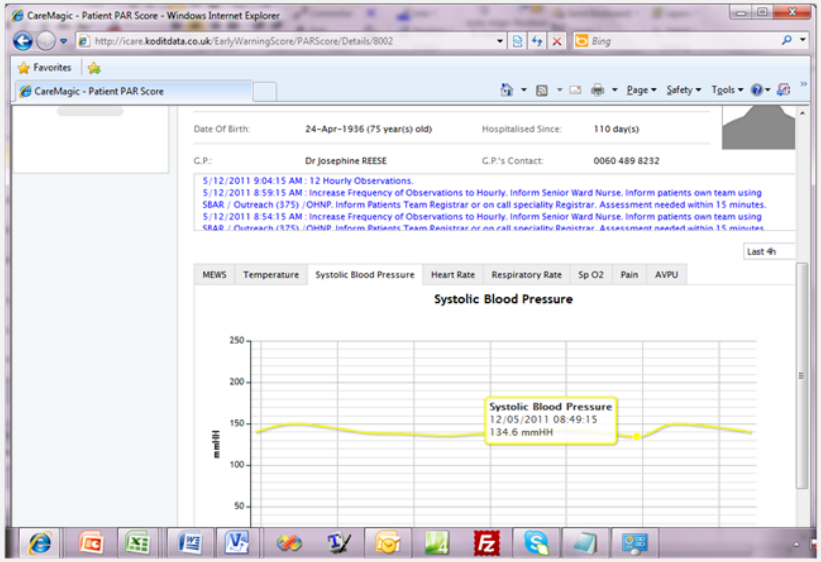
Domain B

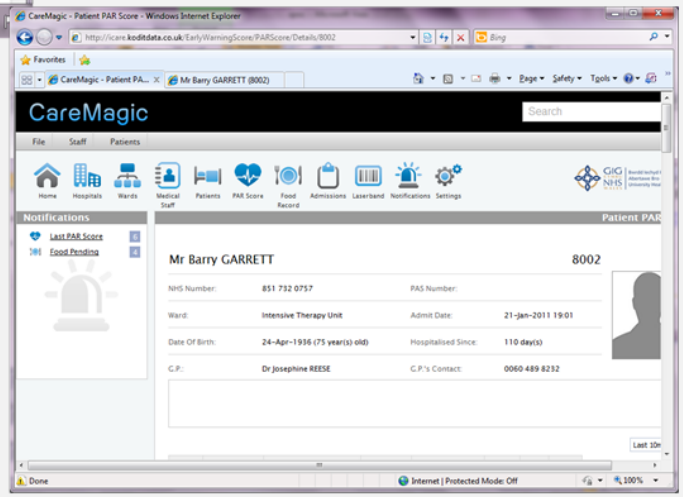
Clinical Services

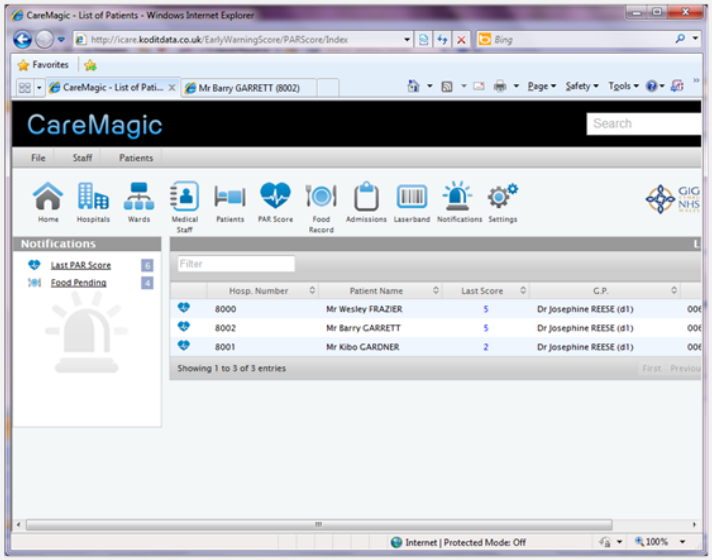


PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab





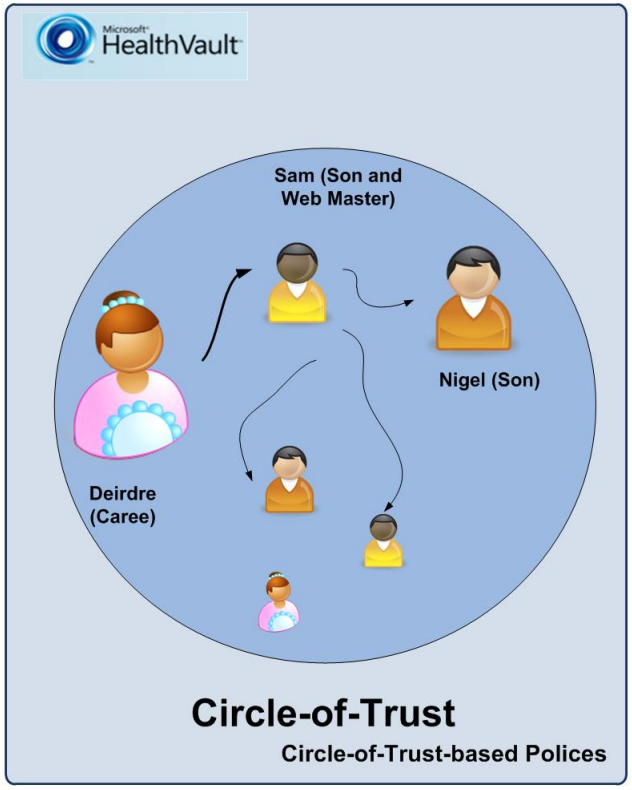




Some screenshots

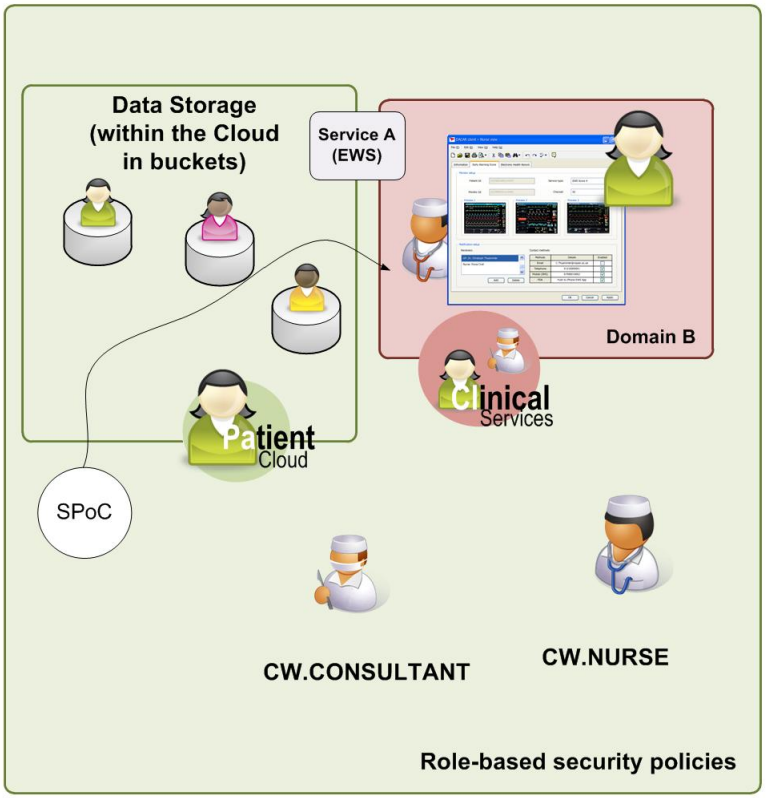
PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab

Assisted Living

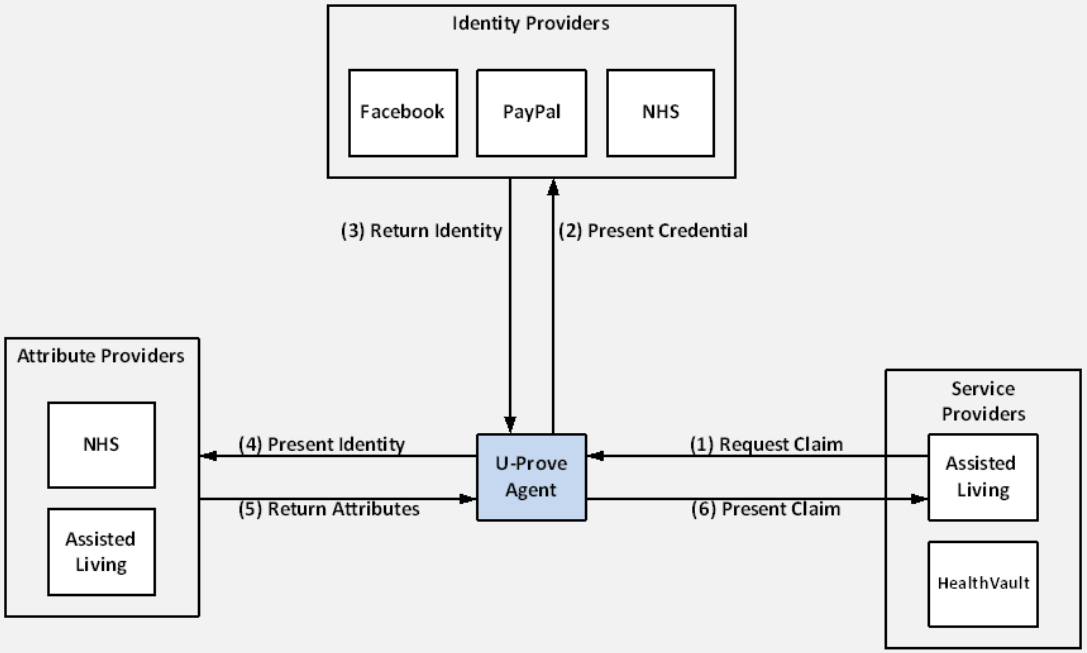


Translation Gateway (Security Policy/ ID Mapping)

Primary/Secondary Care




```
[permit] [C&W.NURSE] [C | R] [Temp | SpO2 | HR | BP | RR | Pain] of [Patient26078] with
[EWS] from [Chelsea & Westminster Hospital] for [*] records in [P2010-12-30T00:00:00] using
[Data Protection Act]

[permit | deny] [Requester] [C | R | U | D] [Attribute] of [Object] with [Context] from
[Owner] for [N] records in [Time Window] using [Compliance]
```



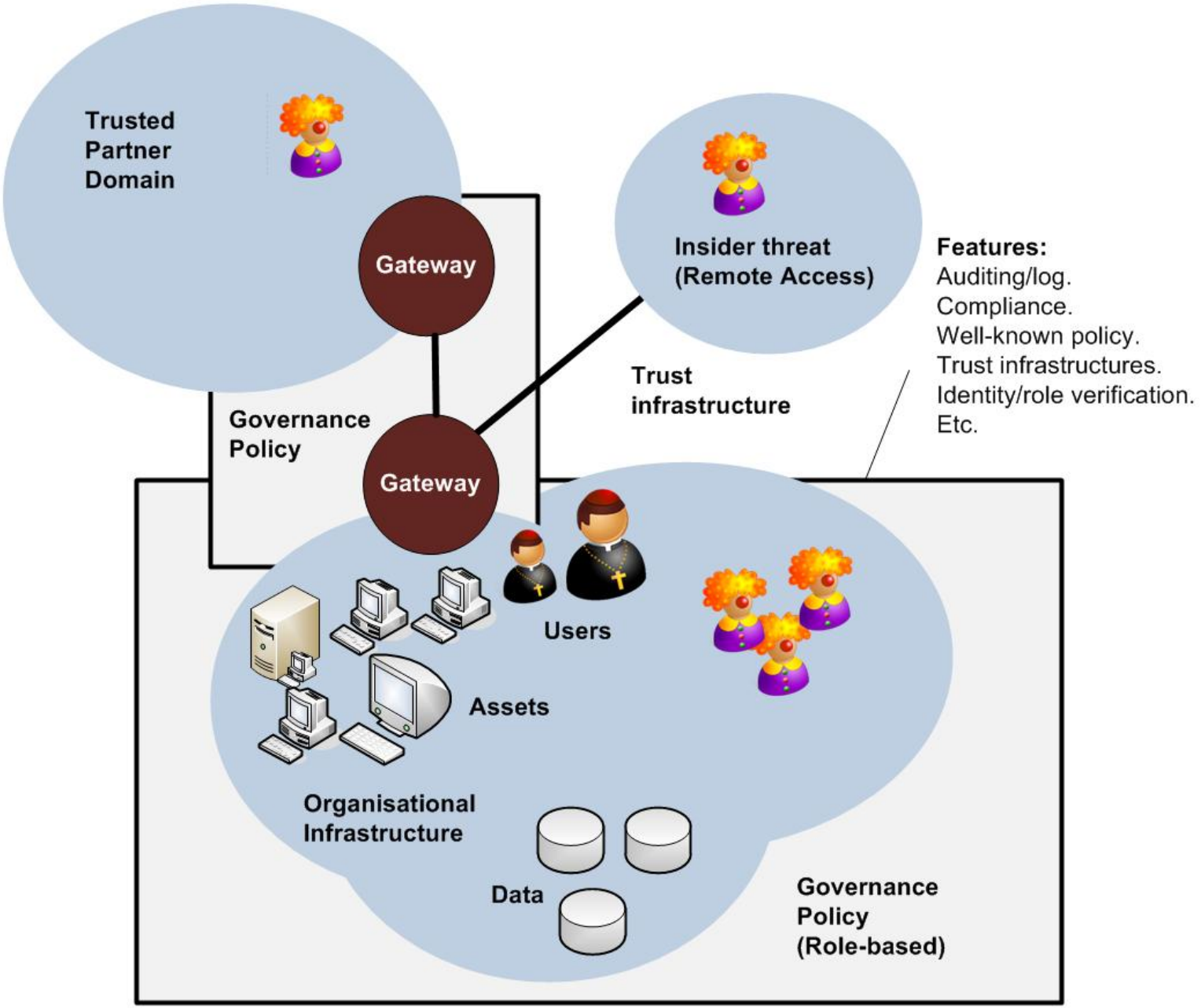
HealthVault

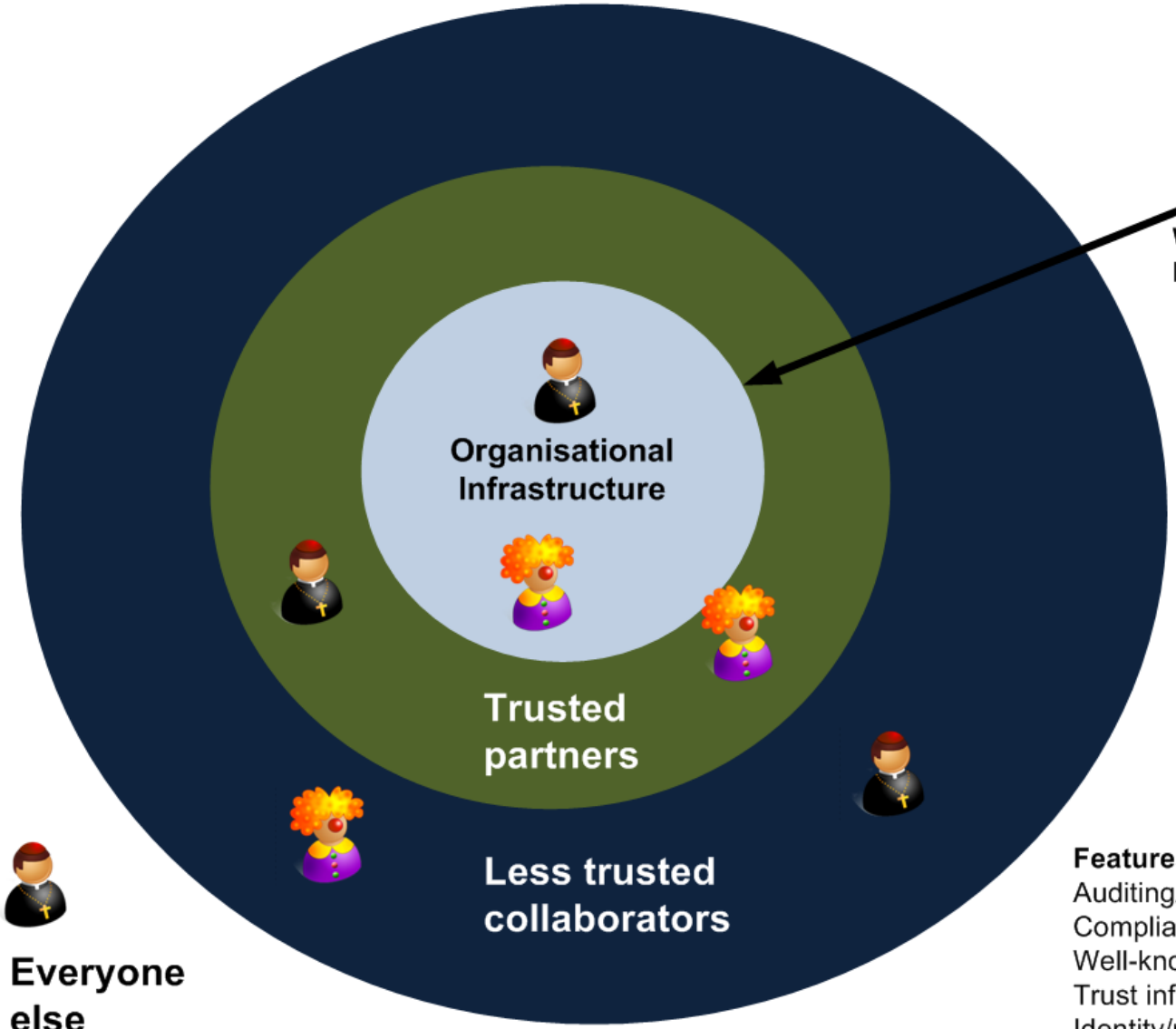
E-Health Platform

CW.CONSULTANT

CW.NURSE

PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab


Trusted
Partner
Domain
Gateway
Insider threat
(Remote Access)
Features:
Auditing/log.
Compliance.
Well-known policy.
Trust infrastructures.
Identity/role verification.
Etc.
Trust
infrastructure
Governance
Policy
Gateway
Users
Assets
Organisational
Infrastructure
Data
Governance
Policy
(Role-based)



Features:
Auditing/log.
Compliance.
Well-known policy.
Trust infrastructures.
Identity/role verification.
Etc.

Insider

BCS

Insider Threat

Technology Strategy Board
Driving Innovation

Alan Bennett

EPSRC
Pioneering research and skills

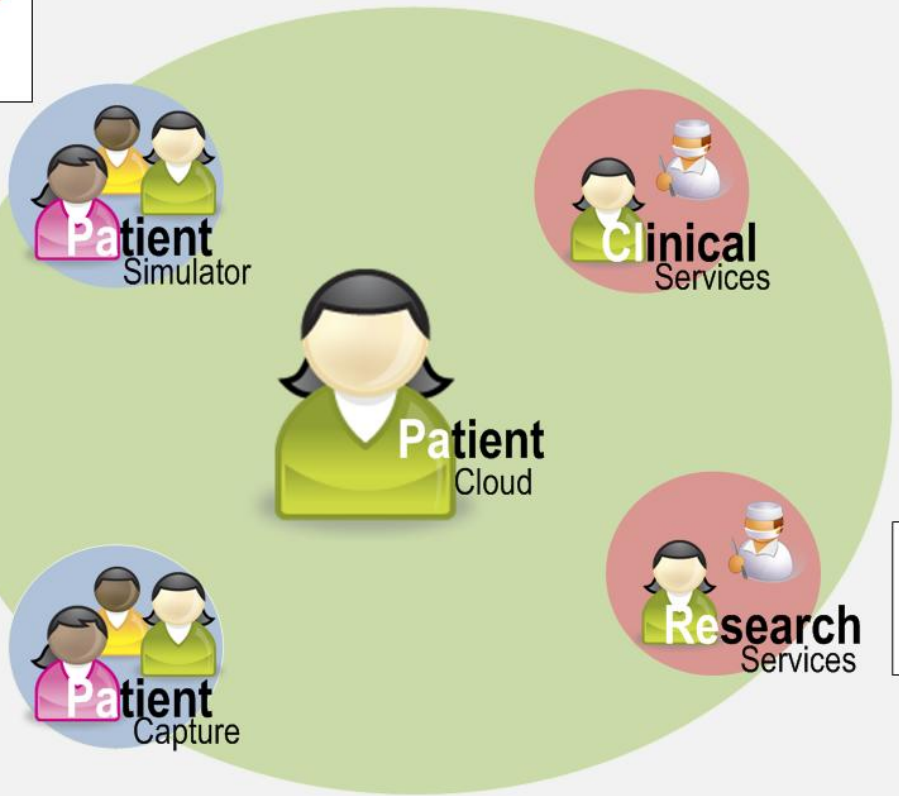
Edinburgh Napier UNIVERSITY

Dr Christoph Thuemmler

Prof Bill Buchanan

Dr Lu Fan

Owen Lo



GS1 UK

Roger Lamb

kodit

Craig Story

Sofyane Khedim

CIPHER LAB

Altaf Sadique

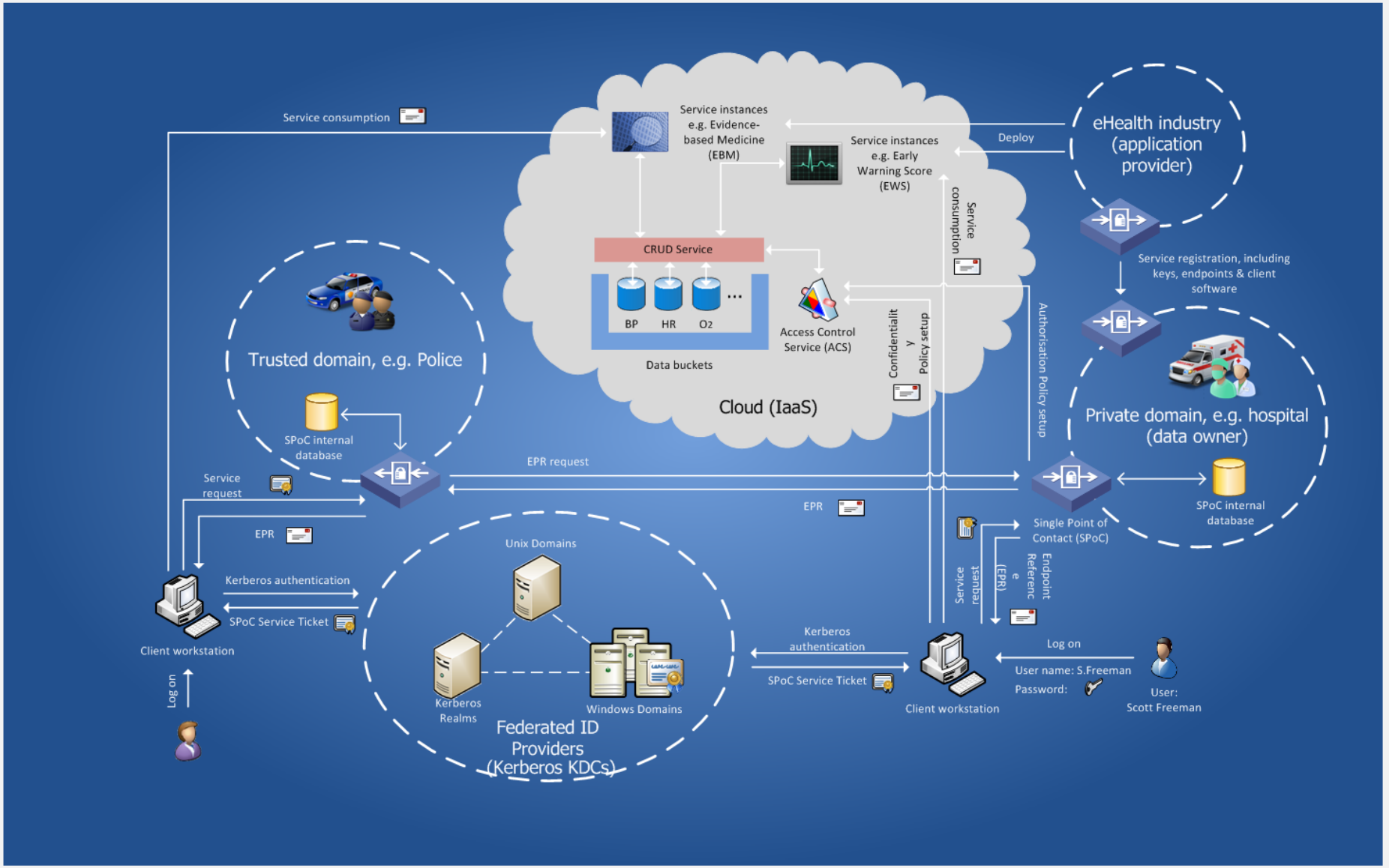
Imperial College London

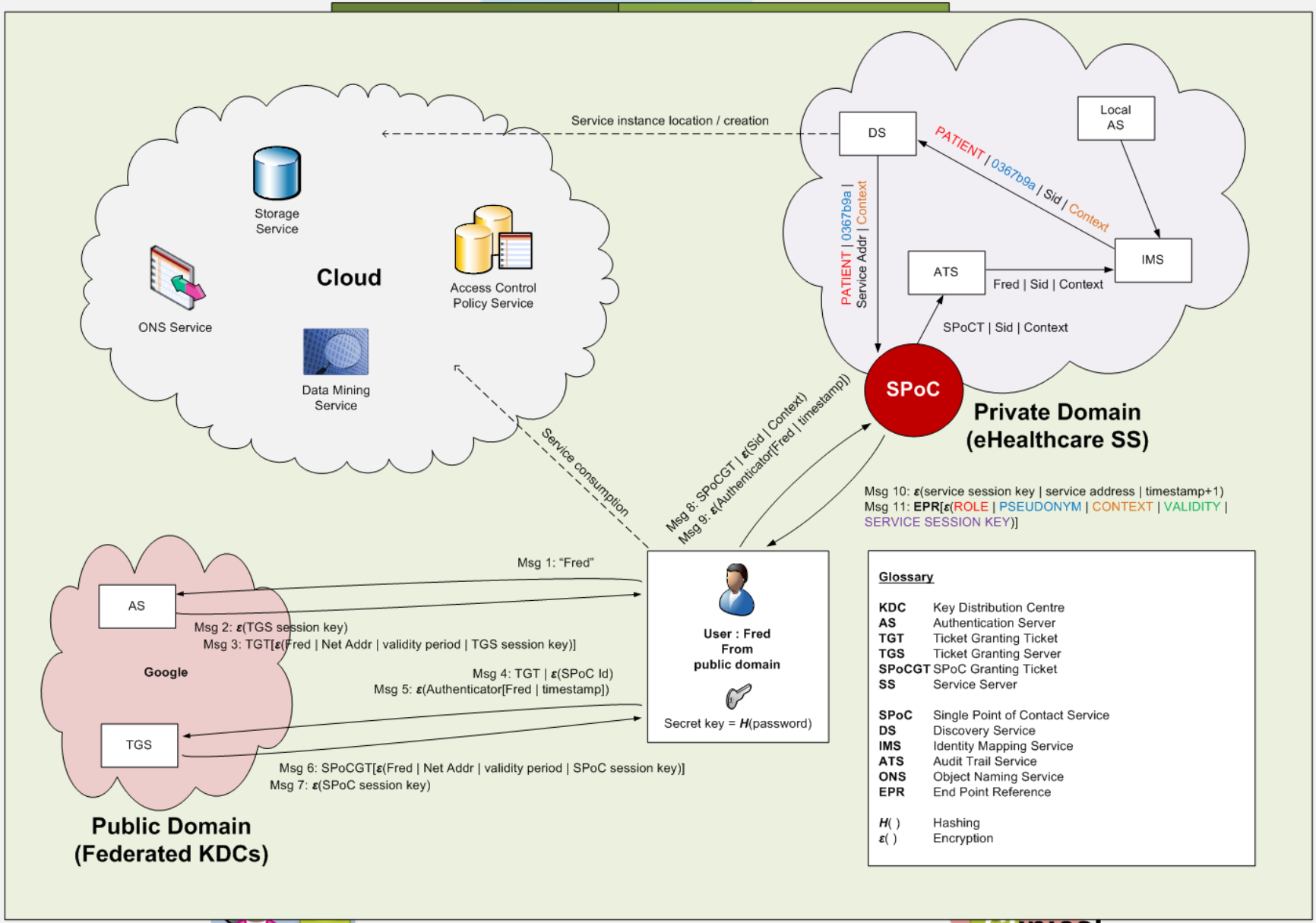
Prof Derek Bell

Ganesh Sathyamoorthy

Chelsea and Westminster Hospital NHS
NHS Foundation Trust

Prof Derek Bell
Tajumal Malik


Service consumption
Service instances e.g. Evidence-based Medicine (EBM)
Service instances e.g. Early Warning Score (EWS)
Deploy
eHealth industry (application provider)
Service consumption
CRUD Service
BP
HR
O2
Data buckets
Access Control Service (ACS)
Confidentiality Policy setup
Authorisation Policy setup
Cloud (IaaS)
Service registration, including keys, endpoints & client software
Trusted domain, e.g. Police
SPoC internal database
Private domain, e.g. hospital (data owner)
SPoC internal database
Service request
EPR request
EPR
EPR
Single Point of Contact (SPoC)
Service request
Endpoint Reference (EPR)
Unix Domains
Kerberos authentication
SPoC Service Ticket
Client workstation
Log on
Kerberos Realms
Windows Domains
Federated ID Providers (Kerberos KDCs)
Kerberos authentication
SPoC Service Ticket
Client workstation
Log on
User name: S.Freeman
Password:
User: Scott Freeman



Patient Simulator

Clinical Services

Integrated Security Policy

PatientCloud:
Funded by EPSRC and TSB, and is a collaboration between C&W, Imperial College, Edinburgh Napier University, Kodit, GS1 and Ciperlab