Access Control

… and a demonstration of

Dave/Dave Master/Master replication

(Dave Evans → Dave Eyers)

Motivating example: a national Electronic Health Record (EHR) service

- (Police and Social Services are similar)
- MUST protect EHRs from journalists, insurance companies, family members etc.
- access policy defined both nationally and locally
- generic scalable policy → **RBAC**
- **exception of individuals** is allowed by law,

  (all doctors except my uncle Fred Smith)

  "Patients' Charter" → **parametrised roles**
- may need to express relationships between parameters

  treating-doctor (doctor-id, patient-id)

Access Control: Requirements / Motivation

- large scale

  → **role based access control (RBAC)**
- potentially widely distributed systemsheterogeneous components, developed independently but must interoperate

  → **service-level policy agreements (SLAs)**

  (which roles authorise their activators to use which services?) negotiated within and between domains
- incremental deployment

OASIS RBAC

- OASIS services name their clients in terms of **roles**
- OASIS services specify **policy** in terms of **roles**

  - for **role entry** (activation)

  - for **service invocation** (authorisation, access control)

  both in Horn clause form

OASIS model of **role activation**

a role activation rule is of the form:

condition1, condition2, ….. $\vdash$ target role

where the conditions can be

- prerequisite role
- appointment credential
- environmental constraint

all are parametrised

OASIS role (continued) **membership** rules

as we have seen, a role activation rule:

cond1*, cond2, cond3*, ….. $\vdash$ target role

role membership rule:

the role activation conditions that must **remain true**, e.g.*

for the principal to remain active in the role

monitored using **event-based middleware**

another contributor to an **active security environment**

OASIS model of **authorisation**

An authorisation rule is of the form:

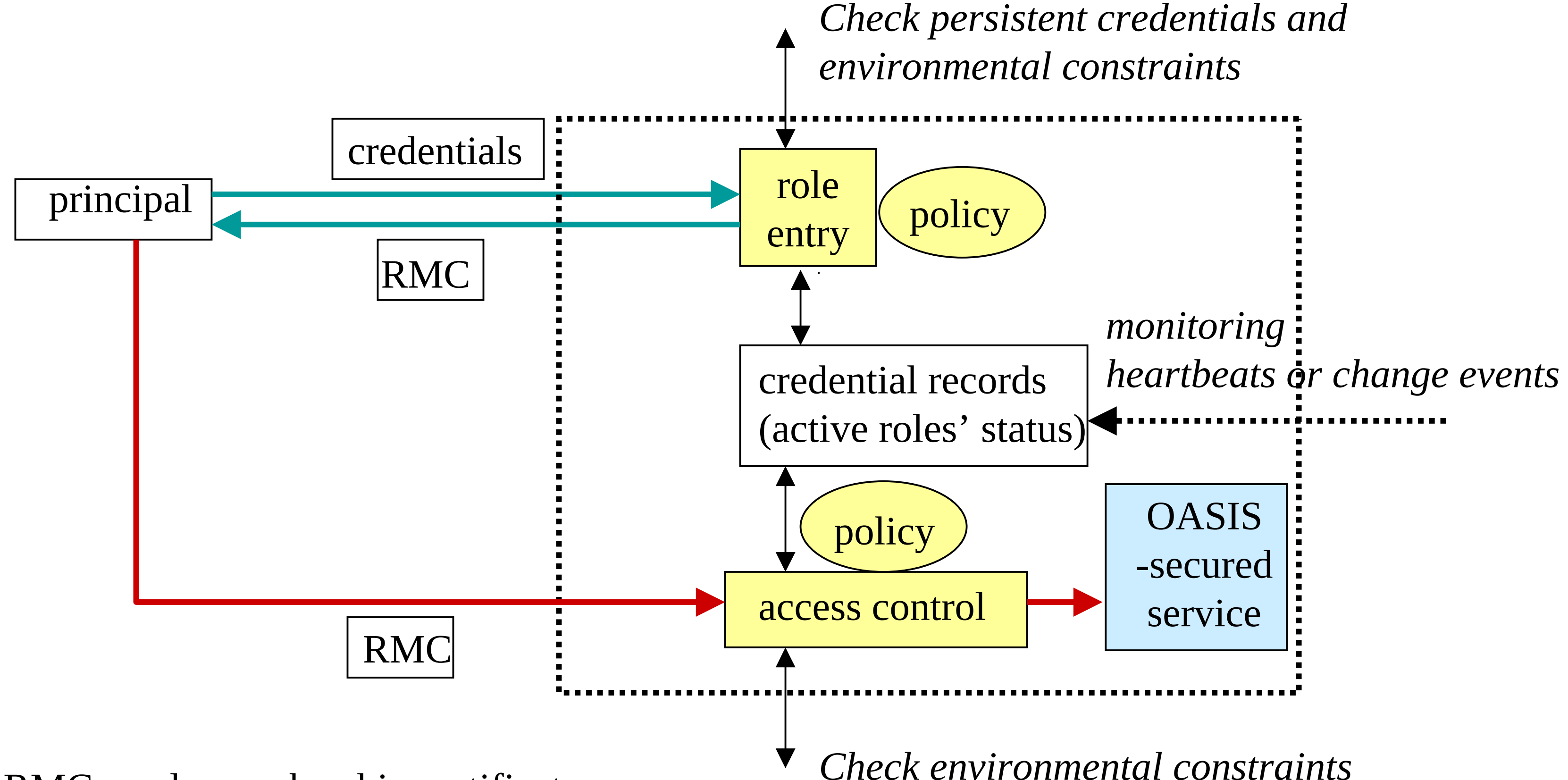
condition1, condition2, ….. $\vdash$ access

where the conditions can be

- an active role
- an environmental constraint

all are parametrised

A Service Secured by OASIS Access Control

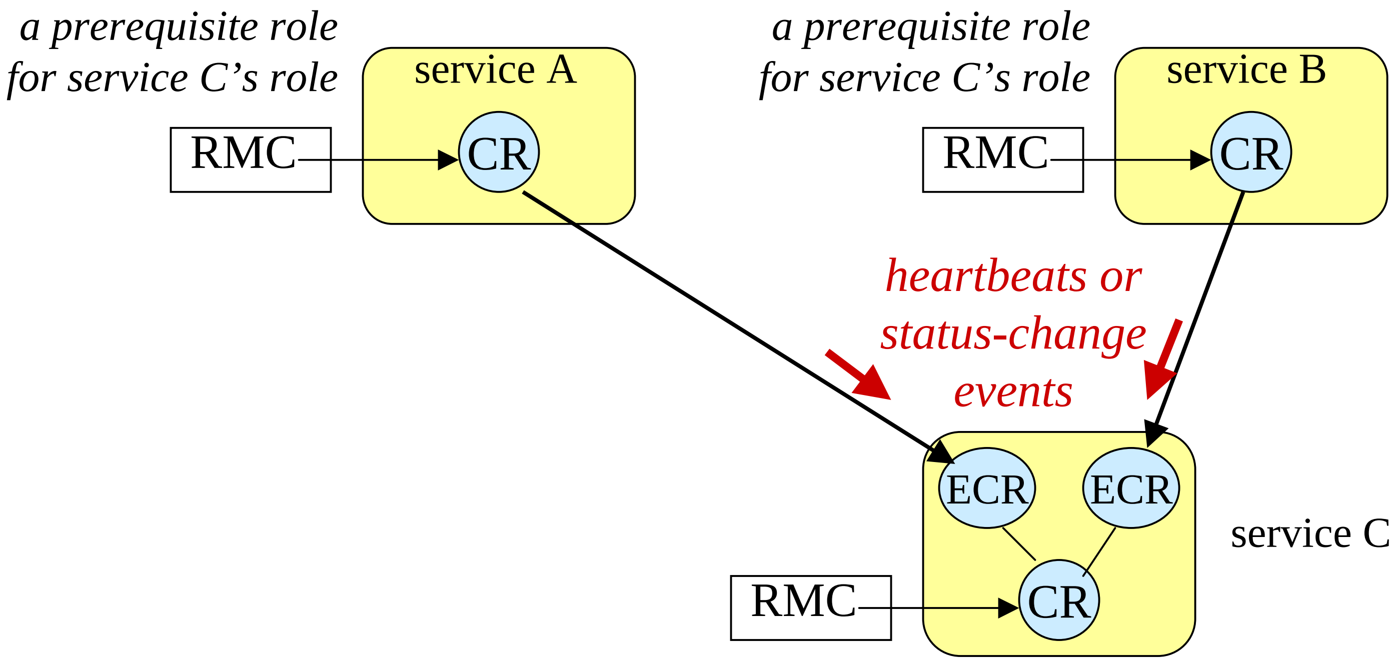

Check persistent credentials and environmental constraints
credentials
principal
role entry
policy
RMC
monitoring heartbeats or change events
credential records (active roles' status)
policy
OASIS -secured service
access control
RMC
Check environmental constraints

RMC = role membership certificate

→ = role entry

→ = use of service

Active Security Environment
Monitoring membership rules of active roles



RMC = role membership certificate
CR = credential record
ECR = external credential record

Roles and RBAC

- naming of roles for scalability, manageability, policy specification *e.g. doctor, sergeant*
- separate administration of people in roles
- parametrised roles for expressiveness: exclusions and relationships *e.g. treating-doctor(doctor-ID,patient-ID)*
- RBAC for access control policy
  for services and service-managed objects,
  (including the communication service)

“all doctors except ……”

“only the doctor with whom the patient is registered for treatment may prescribe drugs, read the patients’ EHR, …”

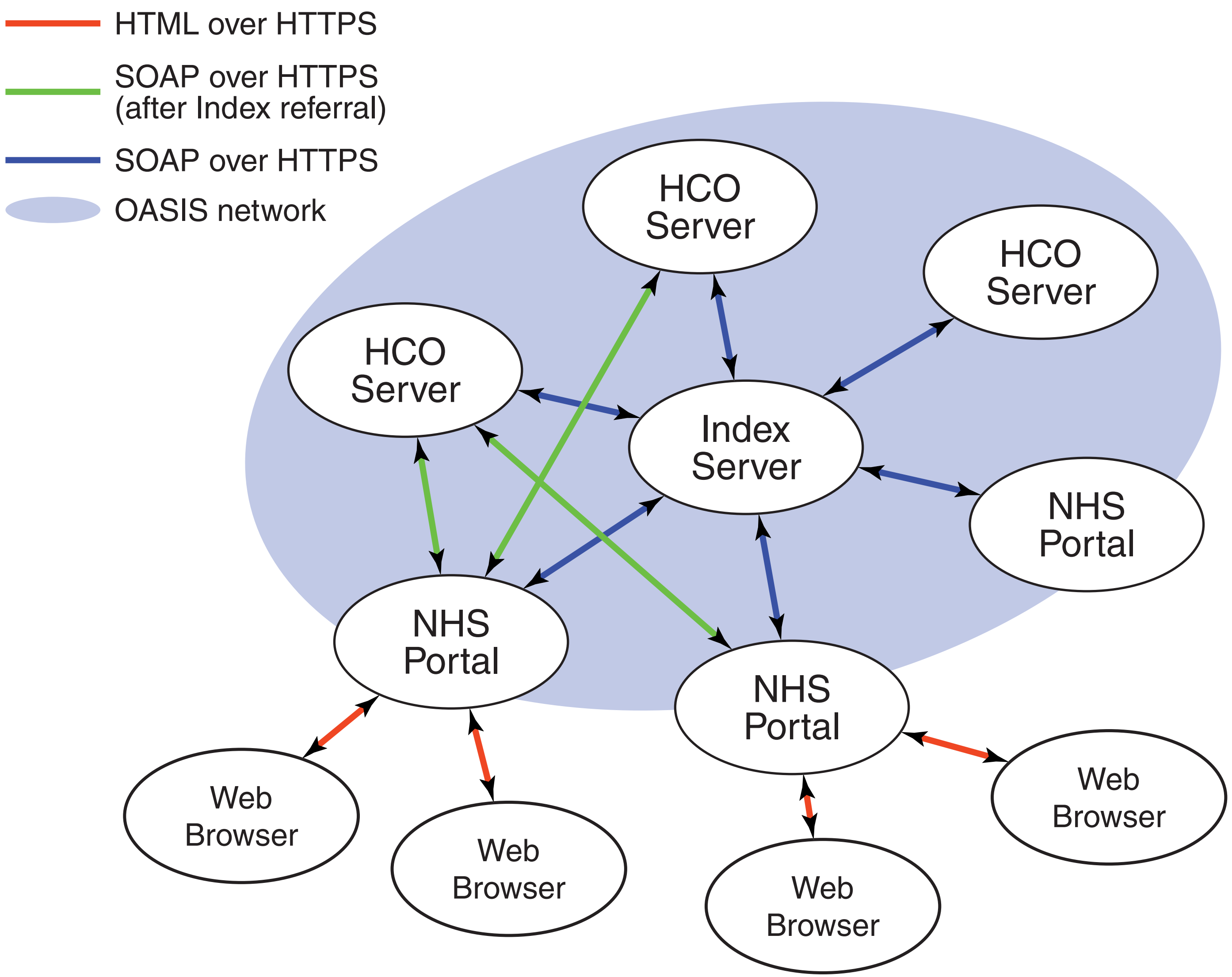
CBCL OASIS applies distributed RBAC

- Prototype EHR system developed in Cambridge

- Three types of (distributed) participants
  - Client browsers
  - Index servers
  - Healthcare organisations

- Index servers were logically central
  - To be implemented as a replicated service

CBCL OASIS prototype (distributed system)



🟥 HTML over HTTPS

🟩 SOAP over HTTPS (after Index referral)

🟦 SOAP over HTTPS

● OASIS network

HCO Server

HCO Server

HCO Server

Index Server

NHS Portal

NHS Portal

NHS Portal

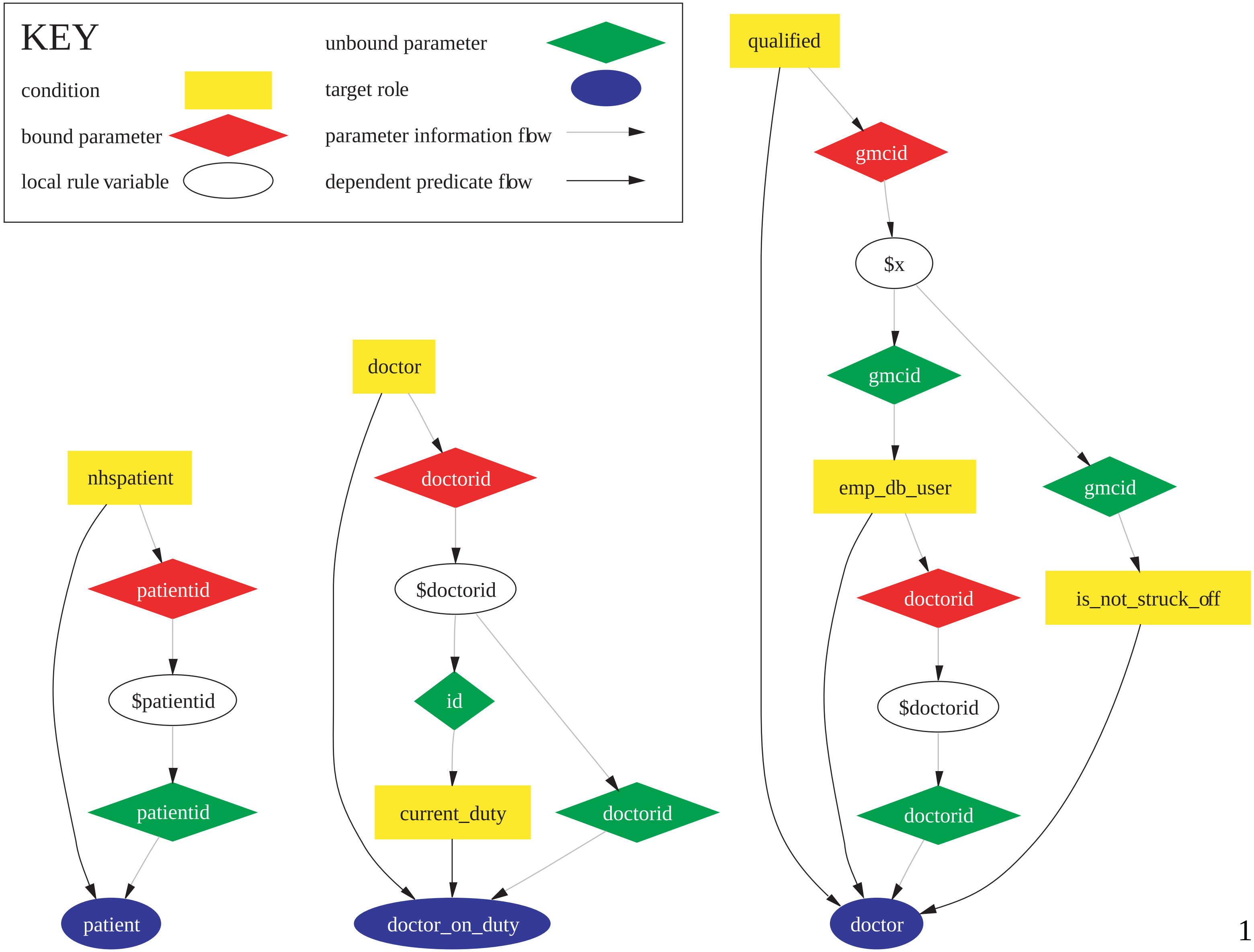
Web Browser

Web Browser

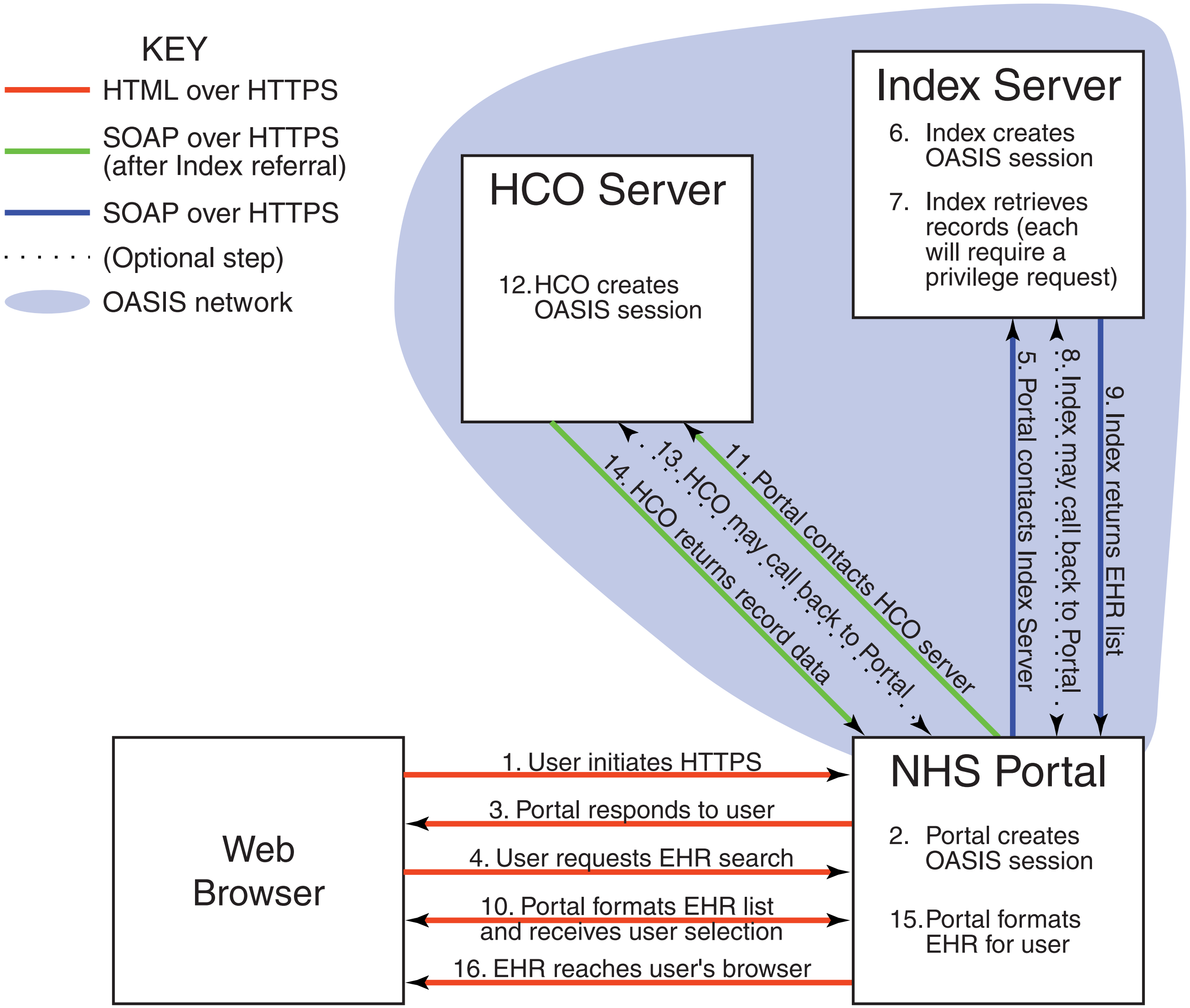
Web Browser

Web Browser

CBCL OASIS prototype (rules)



CBCL OASIS prototype (protocol)



KEY
- HTML over HTTPS
- SOAP over HTTPS (after Index referral)
- SOAP over HTTPS
- (Optional step)
- OASIS network

Index Server
6. Index creates OASIS session
7. Index retrieves records (each will require a privilege request)

HCO Server
12. HCO creates OASIS session

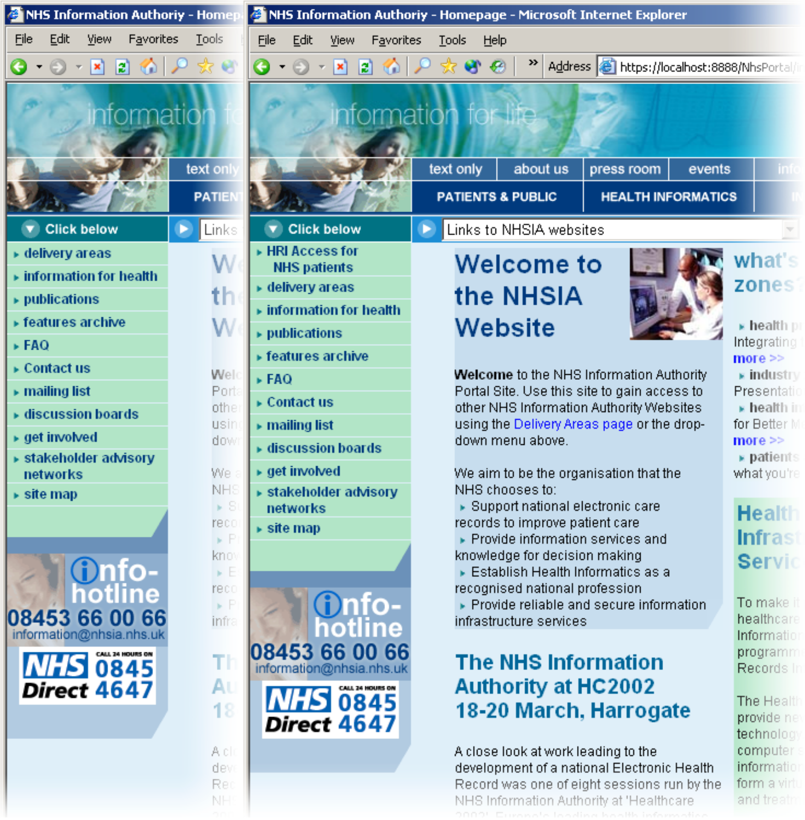
NHS Portal
2. Portal creates OASIS session
15. Portal formats EHR for user

Web Browser

1. User initiates HTTPS
3. Portal responds to user
4. User requests EHR search
5. Portal contacts Index Server
8. Index may call back to Portal
9. Index returns EHR list
10. Portal formats EHR list and receives user selection
11. Portal contacts HCO server
13. HCO may call back to Portal
14. HCO returns record data
16. EHR reaches user's browser

CBCL OASIS prototype (screenshot)

- Menu items make OASIS privilege requests
- Necessary prerequesites might not be known
  - Give too little and fail
  - Multi-round negotations
  - Hand over wallet
- Research is ongoing…



Welcome to the NHSIA Website

Welcome to the NHS Information Authority Portal Site. Use this site to gain access to other NHS Information Authority Websites using the Delivery Areas page or the drop-down menu above.

We aim to be the organisation that the NHS chooses to:

- Support national electronic care records to improve patient care
- Provide information services and knowledge for decision making
- Establish Health Informatics as a recognised national profession
- Provide reliable and secure information infrastructure services

The NHS Information Authority at HC2002 18-20 March, Harrogate

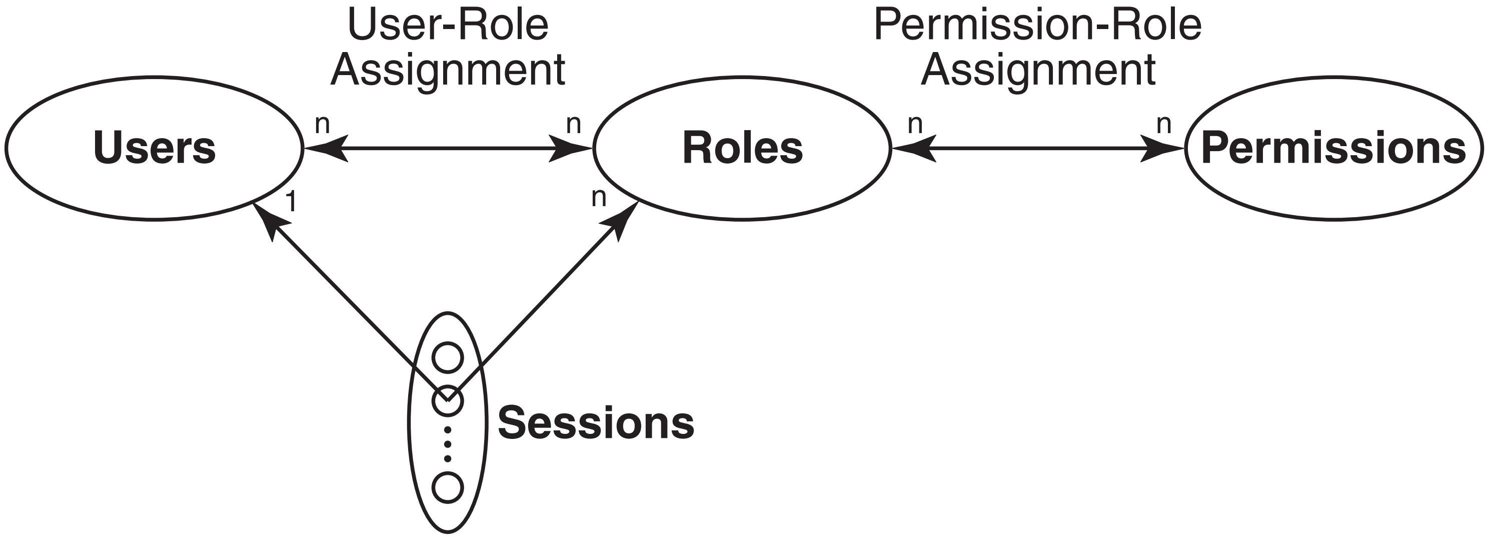
A close look at work leading to the development of a national Electronic Health Record was one of eight sessions run by the NHS Information Authority at 'Healthcare

Microsoft® HealthVault and friends

- … indeed some of that healthcare policy research is being done at MSR Cambridge (Moritz Becker and others)
  - Becker's Ph.D. thesis demonstrates encoding of NHS policy into a Role-Based Access Control framework
  - Employed a form of Datalog with constraint domains
  - Much policy turns out not to need fancy RBAC features
- The big players are scrambling to support e-healthcare
  - Microsoft® HealthVault, Google™ Health, at least
  - Usually focused on giving users control over their own data

NIST provides RBAC standards

- US National Institute of Standards and Technology defines four RBAC reference models
  - RBAC$_0$: users, roles, sessions and permissions (see below)
  - RBAC$_1$: adds role hierarchy
  - RBAC$_2$: adds constraints



You’ve frequently encountered distributed AC

- Raven
- Kerberos
- Shibboleth
  - (well… you may encounter it soon…)

- ZOMG this isn’t in my printed notes!?
- Will this be in the exam?
  - My aim is to illustrate key distributed systems principles by exploring some real-world systems
  - i.e. “No”. Feel free to sleep / meditate / leave / whatever

Raven

- Stem proliferation of passwords for UCam web services
  - Raven is an Ucam-webauth Single Sign On system instance
  - Developed within Cambridge (by Jon Warbrick)

- Three parties in the Ucam_webauth protocol:
  - User's web-browser
  - Target web-server
  - Raven web-server

- Authentication token passed as an HTTP cookie
  - Thus should be passed using HTTPS… but often isn't

Example Raven dialogue

- User requests protected page
- Target web-server checks for Ucam-WLS-Session cookie
- If found, and decodes correctly, page is returned. Done.

- Otherwise, redirect client browser to Raven server
  - Encodes information about the requested page in the URL
- Raven inputs and checks credentials
  - (Also permits users to “cancel”)
- Raven redirects client browser to the protected page. Done.
  - (An HTTP 401 error will be generated if users cancelled)

Raven coordinates participants using time

- Target web-server verifies Ucam-WLS-Session cookie
  - Public-key of Raven server pre-loaded on target web-server
- Target web-server and Raven do not interact directly
  - Client browser receives, stores and resends cookies
- What about malicious client behaviour or interception?
  - e.g. replay attacks?
- Raven requires time-synchronisation
  - A site-specific clock-skew margin can be configured

Raven does authentication, not authorisation

- Compare the previous dialogue with OASIS access control
  - Not utilising RBAC abstractions between user and role!
  - Decisions made on the basis of identity…
- A promising approach is emerging:
  - Use Raven for authentication
  - Use Lookup for authorisation (LDAP)
    - Lookup groups facilitate self-administration
- So now requests for a resource involve four systems…
  - e.g. UCS Streaming Media Service works this way
  - Caching? Consistency problems, etc.

Shibboleth provides federated authentication

- System for federated authentication and authorisation
  - Internet2 middleware group standard
  - Implements SAML: Security Assertion Markup Language
  - Facilitates single-sign-on across administrative domains

- Raven actually speaks both Ucam-webauth and Shibboleth
  - Shibboleth has the advantage of wider software support

- Identity providers (IdPs) supply user information
- Service providers (SPs) consume this information and get access to secure content

Shibboleth exchange

- Similar to Raven, but with some extra indirection
  - User requests protected resource from SP
  - SP crafts authentication request
  - User redirected to IdP or ‘Where Are You From’ service
    - E.g. UK Federation WAYF service
  - User authenticates (external to Shibboleth)
  - Shibboleth generates SAML authentication assertion handle
  - User redirected to SP
  - SP may issue AttributeQuery to IdP’s attribute service
  - SP can make access control decision

OpenID

- Another cross-domain single-sign-on system

- Shibboleth is organisation-centric
  - Organisations must agree to accept other organisations' statements regarding foreign users
  - Lots of support within the UK Joint Information Systems Committee (JISC) for accessing electronic resources

- OpenID is user-centric
  - Primarily about identity
  - OpenIDs are permanent URI or XRI structures

OpenID (cont)

- User provides their ID to relying web site
  - OpenID 1.0 retrieves URL, learns identity provider
  - OpenID 2.0 retrieves XRDS, learns identity provider
    - XRDS/Yadis indirection affords greater flexibility

- Many big commercial players offer OpenID assertions
- Lots of open source software support for OpenID also

- In terms of responsibility, consider use for:
  - Access to a web resource
  - Access to a wireless network