

EnCoRe Publications

All the EnCoRe deliverable and a list of papers are available on the project's [website](#). Papers by E. Whitley and N. Kanellopoulou analyse Privacy and Informed Consent, and University of Warwick has published papers about Policy Refinement Checking and informed revocation.

The [page](#) is constantly updated, so please keep an eye on it - papers about biobank case study will be added shortly.

support future needs such as the ones related to the third case study. The *third EnCoRe Technical Architecture* primarily refines and finalises previous specifications in the following areas: flexible expression of privacy preferences (choices); tracking of data whereabouts; privacy-aware access control policies and obligation policies; sticky policies; logging, auditing and compliance checking. These refinements are driven by additional knowledge and requirements gathered in EnCoRe, during the second and third case studies.

Various use cases, related to the UK Cabinet Office/Identity Assurance Programme, have been taken into account to illustrate how EnCoRe can provide the desired capabilities in terms of dynamic consent and privacy management.

The third Technical Architecture document describes the resulting final EnCoRe architecture. Although inspired by, and focused on, the specifics of the third EnCoRe case study, this architecture is much more widely applicable than to just that scenario, being suitable for use in other scenarios where an individual (the data subject) discloses his or her personal data to an organisation, which may wish to disclose it to other organisations. Its legal ability to do so may depend on the specific details of the consent, granted by the data subject at the time of disclosure. At that time, the data subject may not be fully aware of the implications of granting consent, and/or may select the simplest consent options offered by the organisation. Later, perhaps after becoming more aware of these implications, or having just changed her mind, the data subject may wish to revoke the previously granted consents and be sure that her new wishes will be respected by all the organisations that have (or have access to) copies of the personal data she disclosed. In order for this to happen, a complex set of interactions, between and within the involved organisations, is required. The EnCoRe architecture provides the framework for these.

The third EnCoRe Technical Architecture document also provides clear and refined guidelines towards the implementation of a related technical solution, consisting of secure and self-standing services to support dynamic consent and privacy management within and across organizations.

These guidelines have been taken into account in the HP Labs's EnCoRe Service Framework, which provides a general, reference implementation of the EnCoRe architecture and its core capabilities, as well as a framework to carry out additional research & development activities.

[M. Casassa Mont, S. Pearson, V. Sharma]

that currently govern the biobanking process. However, it is now possible to develop reliable, dynamic processes that can resolve many of these ethical and legal concerns. The 'dynamic consent' approach therefore offers the opportunity to fundamentally transform the process of medical research in a manner that addresses the concerns of both patients and medical researchers and researchers from EnCoRe have been presenting these insights to both ORB and the Department of Health. The results of the analysis will be appearing in a peer-reviewed journal early in 2012.

[E. A. Whitley]

Contact

To contact us, read about the project, get to know the participants and download papers and deliverables, visit the EnCoRe website:

www.encore-project.info

We are Twittering, [Follow us!](#)



HP Labs' EnCoRe Service Framework: a General, Reference Implementation for Dynamic Consent and

WP4

The objective of this work package has been to ensure the integration of technical, procedural and legal approaches to consent and revocation by exploring the existing and likely future regulatory environment. WP4 completed legal and

Privacy Management

HP Labs completed the development of the [EnCoRe Service Framework for the management of dynamic consent and privacy](#) within and across organisations. This framework provides a general, reference implementation of EnCoRe technical capabilities, fully consistent and compliant with the third [EnCoRe Technical Architecture](#).

The HP Labs Service Framework supports four general use cases that apply to all case studies explored in EnCoRe:

- A data subject (end-user) submits his/her personal data to an organization along with the expression of their consent preferences;
- An entity within the organisation trying to access personal data and being constrained (in so doing) by related data subjects' consent preferences and policies. The organization uses EnCoRe to explicitly enforce (privacy) preferences and policies;
- The disclosure of personal data to a third party, along with associated consent preferences, via the sticky policy mechanism;
- A data subject subsequently changes their mind and modifies/revokes their consent. Changes are automatically propagated to all the involved parties;

A fully working prototype has been built by HP Labs, to fully illustrate the capabilities of the EnCoRe Service Framework and the four general use cases.

Specifically, the Service Framework implements the following key EnCoRe Architectural capabilities: module for the configuration of supported Privacy Preferences and Policies; the Consent/Revocation Provisioning module; the Data Registry module; the Privacy-aware Access Control module; the Obligation Management module; Internal and External Workflow Management modules; the Sticky Policy Management module; instantiation of types of Privacy Preferences, various Access Control and Obligation Policies.

The various components of the Service Framework have been implemented to run as self-standing, secure and distributed services within an organisation. The goal is to ensure that early adopters of the EnCoRe toolkits can use this framework to explore its privacy management capabilities and deploy an extended version of it within their IT operational environments. The implementation uses state-of-the-art technologies based on the Java framework. It uses the [REST](#) methodology and approach for a quick and flexible development of service interfaces and the exchange of information between the involved services. The EnCoRe components are implemented as self-standing [RESTful services](#). These service components can be distributed across different IT systems based on needs. Their implementation supports state-of-the-art security, including encryption of data and secure SSL communication. The representation of information that is exchanged between these EnCoRe components uses the XML technology to support future extensions and quick adaptation to the needs of different organisations and their IT operational environments. This framework has been used by HP Labs as a platform for experimentation of innovative privacy management and consent/revocation solutions. Specifically, HP Labs used it to develop and deploy

philosophical research on privacy, consent, and control in the use of personal information and its application in UK law, and mapped the existing law and regulatory environment to the project case studies and, their detailed use cases, to aid the design of the EnCoRe user interface. By providing continuous legal and regulatory input to the other EnCoRe partners, WP4 contributed a detailed understanding of current information law and governance, and it identified where potential gaps exist as, for example, is the case of revocation in UK and EU data protection law. It addressed these gaps by developing, publishing, and disseminating appropriate research papers and policy recommendations. To further assist the design of the case studies, and in collaboration with WP3, WP4 carried out empirical research on privacy, consent, and revocation to gather and analyse requirements for the project case studies. For a current example, please see our update on the EnCoRe/ORB pilot study in this newsletter. WP4 has published its research results in relevant reports and peer-reviewed papers. It also submitted various responses to policy responses on selected issues in data protection and information governance both in the UK and EU, and has been disseminating its research findings to relevant policy and research stakeholders.

[N. Kanellopoulou]

Successful Integration of the Biobanking Case Study

On 25th November the EnCoRe team met with ORB to present the outcomes of EnCoRe Case Study 2, which aims to offer dynamic consent capability for donors and patients. A lengthy discussion surrounding the design, technical integration and compliance issues

advanced solutions for: the tracking of whereabouts of personal data (via an enhanced version of the Data Registry component); the management of sticky policies by means of a variety of possible technical approaches. The service framework now fully supports sticky policies as the mechanism to exchange personal data and privacy preferences across parties, in a safe and accountable way. A reference implementation is available as described in.

The HP Labs Service Framework is also an agile platform to develop demonstrators for a variety of needs, including prototypes of the overall system for the EnCoRe engagement with the [Cabinet Office Identity Assurance Programme](#).

HP Labs are exploring the opportunity to release this Service Framework in the context of an Open Source initiative. This option is currently being discussed within EnCoRe and various involved organisations: a decision will be made towards the end of the project (April 2012).

[M. Casassa Mont, S. Pearson, V. Sharma]

took place.

The trust building benefits of Dynamic Consent are considered important for the future of Biobanking where the patient/donor is kept in informed and in control rather than the current one-way approach which leaves donors, having signed a consent form, isolated and often confused as to what they agreed to.

The User Interface is presented as simple and intuitive series of web pages which enable the patient/donor to view why and where their donations have been used. Most importantly though they are able to identify organizations, research institutes or specific research fields for which the donated samples should be made unavailable – i.e. a revocation of consent. Current, paper based, processes make this almost impossible for a patient/donor to assert.

[D. Lund]



HP Labs' EnCoRe Demonstrator for Cabinet Office/Identity Assurance Programme

HP Labs developed a fully working demonstrator to illustrate the EnCoRe capabilities (for dynamic consent and privacy management) in the context of the UK Cabinet Office/Identity Assurance Programme. This demonstrator fully leverages the [EnCoRe third Technical Architecture](#) and the related HP Labs's prototype based on the [EnCoRe Service Framework](#). The [Identity Assurance Programme](#) aims to deliver a rich ecosystem of services and to use standard federated identity management solutions to enable the relevant interactions between citizens (users), Identity Providers (IdP), the Hub, Attribute Providers and Public/Private Service Providers (PSPs).

Specifically, a citizen, when trying to access an online PSP service, is redirected, via the Hub, to a trusted IdP of choice, where they can be identified and authenticated. The citizen does this by providing their authentication credentials (the type of credentials to be used might change depending on the required level of assurance). Once authenticated at the IdP site, a *Minimum Data Set* (MIDS i.e. basic personal data such as name, surname, etc.) necessary to identify the data subject is passed to the Hub that might enrich it by adding additional information retrieved from Attribute Providers. Finally the Hub passes the MIDS data, along with any additional information, to the PSP, for local matching if identities (i.e. local identification/authentication) and to enable the citizen to access the desired services. The goal is to ensure that the asserted identity of a citizen can be

successfully used at the PSP site, to identify the citizen based on the locally available information. It is important to notice that, in the described scenario, lots of personal data can potentially be exchanged between the various stakeholders, related to authentication, matching (MIDS) and business transactions. *To make this programme successful, it is important that citizens (data subjects) have control over how their personal data is disclosed between the various stakeholders and subsequently used; they must be allowed to change their consent and related privacy preferences at any time; they must have degrees of assurance that their preferences are enforced by the various stakeholders.*

EnCoRe helps to provide citizens with the desired level of control over their personal data and the involved organisations with mechanisms and solutions for enforcing privacy and consent.

The HP Labs' demonstrator illustrates how this can be achieved in practice, by animating the following key use cases:

- Use Case 1: a citizen (data subject) provides consent for the use of their personal data as MIDS
- Use Case 2: a citizen provides consent for the use of selected Attribute Providers for the MIDS matching process
- Use Case 3: a citizen provides consent for sending / using further Verified Attributes
- Use Case 4: ensuring privacy in transactions through the Hub by using sticky policies
- Use Case 5: changing and propagating data & consent updates
- Use Case 6: a citizen revokes consent for an IdP to hold their data at all

The demonstrator uses the HP Labs' EnCoRe Service Framework (and prototype, deployed via an EnCoRe toolbox) within 3 simulated environments: an IdP, the Hub and the Service Provider.

The demonstrator focuses on the viewpoint of end-users (citizens), administrators and employees. It illustrates how dynamic consent and privacy management can be achieved in this context.

HP Labs are available to provide demos to illustrate EnCoRe capabilities in the context of the Identity Assurance scenario and other scenarios.

[M. Casassa Mont, S. Pearson, V. Sharma]

Subscribe and unsubscribe

To subscribe or unsubscribe, send an email to encore-newsletter-owner@lists.hpl.hp.com

Your email address will be stored securely and used only for distribution of this newsletter.

The EnCoRe website Privacy Policy is available on the [website](#).



Ensuring Consent and Revocation: Mapping the Views of Patients, Researchers, and Clinicians in the Oxford Radcliffe Biobank

This pilot was the project's second case study to gather requirements for the management of data in biobanking, and in particular biobanking to collect and analyse users' views on the nature and scope of consent, desirability of notification, revocation, and other system functions relevant to

the design of the EnCoRe user interface. In addition to reviewing user attitudes towards biobanking in existing research literature, the project obtained the required research ethics and NHS Trust management approvals and conducted a qualitative study with patients, researchers, clinicians who are involved in the Oxford Radcliffe Biobank (ORB).

While much is known about patient attitudes to ethical and legal questions in the context of biobanking, particularly regarding privacy protection and consent, little is known about the attitudes of medical researchers who use biobanks for research to these issues. EnCoRe therefore ran four focus groups with medical researchers associated with the Oxford Radcliffe Biobank in 2010–2011. Analysis of the transcripts from the focus groups highlights a range of issues associated with the research oversight and consent process, including obtaining ethical approval to use biobank samples and particular concerns for international studies; the benefits and limitations of broad consent; and the possibilities of revoking consent. EnCoRe's approach to these issues suggests that many of these issues originate in the relatively static consent processes that currently govern the biobanking process. However, it is now possible to develop reliable, dynamic processes that can resolve many of these ethical and legal concerns. The '*dynamic consent*' approach advocated by EnCoRe offers the opportunity to fundamentally transform the process of medical research in a manner that addresses the concerns of both patients and medical researchers. Researchers from EnCoRe have been presenting these insights to both ORB and the Department of Health. The results of the analysis will be appearing in a peer-reviewed journal early in 2012.

More information on the EnCoRe/ORB pilot study is available at:

<http://www.publichealth.ox.ac.uk/helex/events/new-encore-orb-pilot-study>

[*N. Kanellopoulou*]