



EnCoRe News August 2011

To access the hyperlinked material, read this newsletter online at <http://tinyurl.com/3mowrrk>

Scroll through this issue to find the following...

[The EnCoRe R&D Service Framework for Privacy Management](#)

[HP Labs, Research and Development related to Sticky Policies](#)

[8th FTRA International conference on Secure and Trust Computing data management and Applications \(STA2011\)](#)

[EnCoRe and the Identity Assurance programme](#)

## Tags

## Focus

## EnCoRe Milestones



### The EnCoRe R&D Service Framework for Privacy Management

HP Labs are developing an R&D Service Framework for the management of Consent/Revocation and Privacy, in the context of the EnCoRe project.

This work aims to provide a flexible, general purpose, agile and extensible R&D platform to further support the exploitation of EnCoRe technologies and solutions. We envisage using this Service Framework in the context of the EnCoRe engagement with the Cabinet Office, in their Identity Assurance Programme.

On 17th August 2011, the EnCoRe implementation proved itself worthy.

In a meeting held at HW's offices in July, WP5 (Compliance) and WP6 (Implementation) came together to agree a format for testing the core logic of EnCoRe's consent management controls. The process defined, allows for an extensible suite of testcases to be developed which can fully reset, configure and test the consent enforced access controls

provided by the the EnCoRe core. This also includes testing the capabilities of notification, auditing, data sharing and flowdown of changed data subject consents and choices to shared data. This activity is in perfect line for validation of the EnCoRe core implementation which is now available as a fully integrated and operational prototype.

-

First of all, the framework aims to provide a general, reference implementation of the EnCoRe Architecture[1,2] including: 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. All these modules can be run as self-standing, secure and distributed services within an organisation. This implementation reflects, in a more general way, the components defined in the architecture and avoids having to make strong compromises to legacy systems. 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.

In this context, the Service Framework illustrates how to support four general key use cases: a data subject (end-user) submitting his/her personal data along with the expression of their consent preferences; a data subject subsequently changing their mind and modifying/revoking their consent; 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 disclosure of personal data to a third party, along with associated sticky policies.

---

## 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](http://www.encore-project.info)

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

---

Secondly, this Service Framework aims to provide a platform to HP Labs (and EnCoRe partners) for experimentation about innovative privacy management and consent/revocation solutions. Specifically, HP Labs are planning to use it to develop and deploy 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. It will allow HP Labs to experiment with more complex scenarios than the ones investigated in the two current EnCoRe Case Studies (that are quite constraining). For example, we can consider more complex and richer interactions between multiple parties.

Thirdly this Service Framework aims to provide a quick and agile platform to develop demonstrators for a variety of needs, including early prototypes of the overall system for the EnCoRe engagement with the Cabinet Office Identity Assurance Programme [3].

Finally, this Service Framework can be used as the foundation of an Open Source release of the EnCoRe toolkits. This option is currently being discussed within EnCoRe and various involved organisations: a decision will be made towards the end of 2011.

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



The EnCoRe team wish you a nice summer - wherever you go... remember don't forget about your privacy.



## HP Labs Research and Development related to

### Sticky Policies

HP Labs has been researching sticky policy mechanisms and how they may be used within the EnCoRe project to help propagate, enforce and audit users' consent and revocation choices along the service provision chain. When personal data passes organisational boundaries, the risk of inappropriate usage or exposure, whether deliberate or accidental, greatly increases. To mitigate this risk, technical mechanisms are needed, in addition to legal agreements and contracts, that enforce the wishes of end users and of organizations acting on behalf of customers or employees regarding the way in which that information is used. We have been researching how 'sticky policies' can help provide a technical solution by means of a user-centric control mechanism involving machine-readable policies (defining allowed usage, disclosure criteria and associated obligations) that are attached to data and travel with it as it is passed among multiple parties. In other words, sticky policies are conditions and constraints attached ('stuck') to data that describe how that data should be treated. Depending on the degree of the policy stickiness, the involved data might be encrypted and access to their content in clear allowed only upon the satisfaction of these policies. In this context a key role is played by Trust Authorities (TAs): these entities provide assurance by keeping track of promises made by the involved parties, related to constraints specified within the sticky policies, in order to access data, along with controlling such access to data. This approach is suitable for enhancing privacy management in a broad range of domains, and particularly in sectors like healthcare, where sensitive information is involved, or to provide privacy protection in the cloud.

Our general approach is as follows, with respect to the EnCoRe architectural components: part of the user privacy choices are embedded into sticky policies by the User Consent and Revocation Assistant to ensure that they will be fulfilled by third parties receiving the data; the Privacy Enforcement and Obligation Management component enforces sticky policies associated with data along with any other policies mandated by the organisation; the External Workflow Manager interacts with the Data Registry to update data locations and related

consent information, and to control onward flow.

The sticky policies sent out from the EnCoRe system to other organizations specify the purposes of using the data and any obligations and prohibitions (including notification and deletion after a certain time), that have been specified by the user in their C&R preferences associated with that data. The Trust Authority functionality is distributed in the sense that the EnCoRe External Workflow Manager component controls sharing of the information associated with the sticky policies, and the Data Registry records how it has been distributed. Optionally, an external TA can also be involved to perform some additional checks if the External Workflow Manager is not able to make those directly.

At the receiving party side, if EnCoRe enabled, there is a translation of the requirements expressed in the sticky policies into access and obligation policies into local access control and obligations policies to be enforced, along with the original data subjects' privacy choices. If the receiving parties do not have EnCoRe compliant systems, then the External Workflow Manager assesses the extent to which the data may be released for a given purpose and controls release of the data accordingly, potentially sanitizing it if needed.

In order to revoke consent, the users use the same mechanisms to edit their consent preferences as those they used to set them in the first place, i.e. via web-based User Interfaces: these preferences are automatically propagated throughout the EnCoRe system as well as beyond it, in a batched manner, to the other organizations involved, by leveraging the information stored in the Data Registry.

This approach can be applied recursively, for a chain of organizations disclosing information between them.

---

We have already surveyed existing techniques for sticky policy functionality and extended this to develop the core mechanisms for the management of sticky policies within the EnCoRe project and are currently implementing a PKI-based implementation of the required mechanisms.

*[S, Pearson, M. Casassa Mont, R. Saeed]*

---

### Subscribe and unsubscribe

To subscribe or unsubscribe, send an email to [encore-newsletter-owner@lists.hpl.hp.com](mailto:encore-newsletter-owner@lists.hpl.hp.com)

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

---

**STA 2011** 8<sup>th</sup> FTRA  
International Conference  
on Secure and Trust  
Computing, data  
management, and

## Applications (STA 2011)

The STA 2011 conference addressed the various theories and practical applications of secure and trust computing and data management in future environments and was the first conference after the merger of the SSDU, UbiSec and TRUST symposiums. It was held at Loutraki, Greece from 28<sup>th</sup> until 30<sup>th</sup> June 2011.

As part of the conference, a one-day Security and Trust for Applications in Virtualised Environments (STAVE) workshop was held in order to focus on policy management issues within the cloud. This was of particular interest to EnCoRe as our mechanisms can apply in this context. Issues addressed by the conference included:

- Compliance with legal frameworks for data protection and privacy
- Identity management between different governmental services
- Security and trust aspects of using virtualisation in a distributed environment
- Policy mapping
- Management of risks and policy compliance verification.

Siani Pearson (from EnCoRe) gave two presentations and chaired half the workshop. Her first presentation was on how accountability in the cloud can be enhanced via sticky policies, and this included discussion of what EnCoRe is and how we are implementing sticky policy techniques within EnCoRe. The co-authors on this paper were Marco Casassa Mont and Gina Kounga. Her second presentation described how natural language techniques can be classified, and furthermore used in a repeatable lifecycle linked to automated policy enforcement. Again, it was explained how EnCoRe-related mechanisms may be used as part of this process. The co-authors on this paper were Nick Papanikolaou and Marco Casassa Mont.

There were a number of other papers presented of interest to EnCoRe, particularly relating to work carried out on policy management within the EU PASSIVE project.

Further details about the conference and workshop may be obtained via <http://www.ftrai.org/sta2011/> and <http://ict-passive.eu/stave/> respectively.

*[S. Pearson]*



### EnCoRe and the Identity Assurance programme

Researchers from various partners in the EnCoRe project are contributing to the UK government's programme, led by the Cabinet Office, to design and deploy a national framework for assuring identities. This will form the basis, over the coming few years, for authenticating citizens' rights of

personalized access to a variety of national and local government online services, and is being designed to be useable for access to services provided by the private sector too.

Unlike the National Identity Scheme proposed by the previous government, this scheme is being set up around a distributed system architecture that accommodates multiple levels of assurance and uses only that personal data which is necessary for the level being sought. Nevertheless, it still poses privacy issues and requires careful assessment of its internal information flows and the governance of these. The management of the lifecycle of consent, by individuals, to the use of their personal information within this framework, is one such issue.

EnCoRe researchers are particularly qualified to assist the Cabinet Office in its work to verify that the technical design of the system architecture, and the propositions on which the framework it implements are based, are appropriate to the needs of the entities that will rely on the assured identities, to citizen users both at a societal and individual level, and to the entities that will provide the assurance. We are taking part in two workstreams within the Cabinet Office's review process that precedes the publication of their intentions for public consultation. One is Technical Architecture and the other is Legal Framework. This review process is expected to complete by the autumn.

EnCoRe has taken great care, in making our technical and process design decisions, to enable and encourage implementation and deployment of our approach to consent lifecycle management by both new and legacy systems that process personal data. For example, we have factored interoperability with user-centric identity management systems into our designs. We understand that the Identity Assurance programme will aim to adopt similar principles to these, and so we are confident of the compatibility of EnCoRe's approach with this programme. We hope, therefore, that it will form one channel for exploitation of our work to the benefit of the UK.

[P. Bramhall]

---

The EnCoRe Project receives funding from the UK Government's *Technology Strategy Board*, *Economic and Social Research Council* and *Engineering and Physical Sciences Research Council*.