An Integrated Cloud-based Healthcare Infrastructure

E. Ekonomou, L. Fan, W. Buchanan, C. Thüemmler
School of Computing
Edinburgh Napier University
Edinburgh, United Kingdom
{e.ekonomou, l.fan, w.buchanan, c.thuemmler}@napier.ac.uk

Abstract—**We present a cloud-based healthcare system that integrates a formal care system (DACAR) with an informal care system (Microsoft HealthVault). The system provides high levels of security and privacy within a cloud environment, enabling sharing of both health records and the access rights, along the patient pathway. We also define a case study that can help in evaluating and in demonstrating the usefulness of a cloud-based integrated health care system.**

Keywords; e-Health Care, Formal Health Care, Informal Health Care, Security, Ambient Assisted Living, Cloud Computing, Service Oriented Architecture

I. INTRODUCTION

Although much research effort has been put into the design and development of novel e-Health services and applications, their interoperability and integration remains a challenging issue [1]. Firstly, health services deal with large amounts of private data which needs to be both fully protected and readily available to clinicians who need to use it [2]. Health care providers often lack the capability to commit the financial resources for either the research or the infrastructure required [3]. In addition, the public is often skeptical about whether IT systems can be trusted with private clinical information. Past failures have fuelled a culture to restrict any innovation by both members of the public and the politicians responsible for health services [4].

Health care systems need to provide strong security and privacy and there have been many attempts to define the security requirements and standardize them [2, 5, 6]. E-Health systems need to be secure in order for patients to trust them, and in order to be legal, as security and privacy are legal requirements in many countries, including the UK [7] and the US [8]. On the other hand, and regardless of reality, cloud computing is not considered trustworthy and secure enough for sensitive e-Health applications. A carefully designed, secure, system needs to be in place before we can argue on the potential of cloud computing in revolutionizing health care.

Our work aims to integrate the DACAR e-Health platform [9] with Microsoft HealthVault to form an e-Health platform that extends across all health care domains. We provide solutions to the problems associated with (a) data security; by carefully integrating already secure subsystems, (b) sharing; by allowing a great degree of both health record and access rights sharing and (c) privacy; by letting the patient retain full control of the access rights to their health record. Our solution is flexible and deployable in a number of cloud infrastructures, giving its operators a variety of options to balance their security and financial requirements.

A. Paper organisation

Brief background to health and e-Health systems is discussed in Section II. Section III outlines the case study. Section IV presents the system design and Section V evaluates it. Finally, Section VI discusses the conclusion and future work.

II. BACKGROUND

A. Healthcare domains

There are two main healthcare domains: *formal care*, referring to institutionalized and centralized health services like hospitals and *informal care*, referring to de-centralized care, mainly for chronic conditions and the elderly population. For example in the UK, formal care consists of NHS central services like Hospitals, while informal care includes private clinics, *Assisted Living*, care at home by relatives and long-term care homes for the elderly.

B. Literature review, related systems and other work

Technology-driven innovation in e-Health systems has introduced the concepts of centralized Electronic Health Records (EHRs) and patient-centric Personal Health Records (PHR) [10]. The PHR provides freedom of capture, storing and sharing to the patient and is more consistent with modern technological trends, i.e. your data is always with you, as well as more similar to the traditional health record keeping in physical copies. In addition to HealthVault, a popular PHR system is Google Health [11] but, unfortunately, it has been discontinued. The Continua Health Alliance [12] device compatibility standards are good alternatives to the device ecosystem of HealthVault. EHR proposals include the work in [13] which proposes to share EHRs among multiple e-Health communities over a peer-to-peer network, traditional IT solutions [14], private clouds [15] and Desktop Virtualization [18]. Finally, the German electronic Health Card (eHC) [17] proposes a distributed system, but is allegedly insecure [16].

C. Overview of DACAR

Figure 1 illustrates DACAR [9], a solely cloud-based e-Health Platform developed at Edinburgh Napier University (ENU). The key contribution is a highly flexible security policy able to control access and sharing of the health records, which in turn are stored in encrypted data buckets.

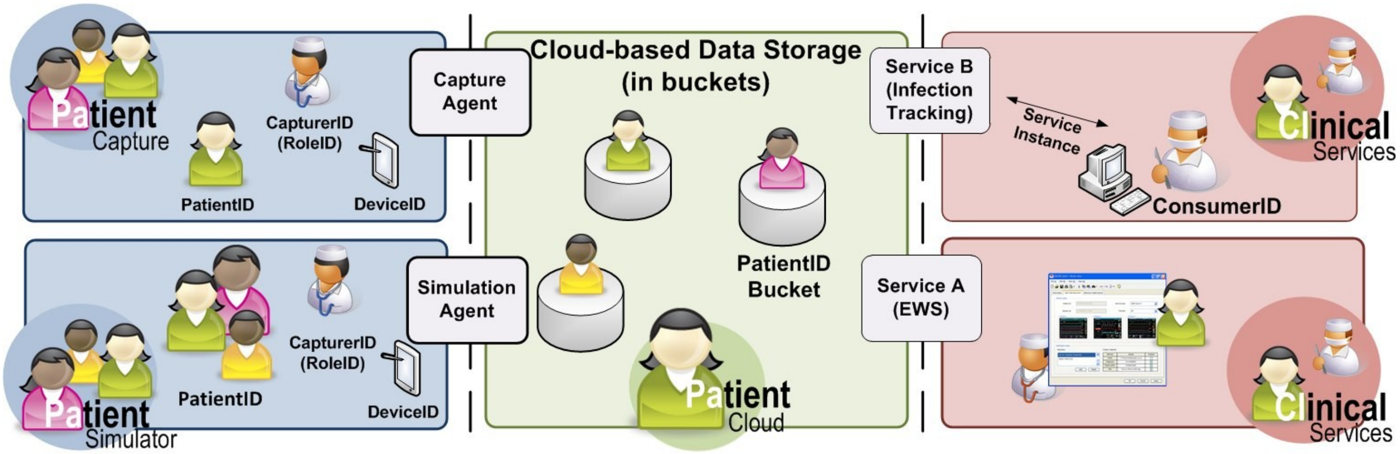

Figure 1: Overview of DACAR showing data capture, simulated capture, cloud storage in buckets and services.

DACAR focuses on providing clinical services, like the CareMagic [19] product implementing the Early Warning Score (EWS) service, to clinicians and other entities where sharing can be defined. DACAR's access control mechanisms are enforced by one or more Single Point(s) of Contact (SPoCs) which are gateways for information exchange. This enables a greater degree of sharing with other domains, such as to social care. The e-Health platform thus provides well-managed clinical services, where there is no direct access to the core data. Currently, the DACAR subsystem supports authentication via Kerberos [20] and requires an account to exist for each user. Users are assigned to one or more roles, e.g. patient, doctor, nurse, etc, and the SPoC enforces user-based, role-based or service-based authorization before it allows them to access a service.

D. *Overview of HealthVault*

Microsoft HealthVault is a cloud-based platform enabling health record management. It follows the Personal Health Record (PHR) model, where a patient is provided with the needed tools to have full control of the creation, storage and sharing of their own health records. For data creation, it supports a range of compatible devices, its device ecosystem, giving users the ability to use home health monitoring devices to store results in HealthVault directly. HealthVault provides a user interface allowing users to review their health data, manage their account, and to define data sharing relationships. These can be set up to be a simple read access up to full custodian access. Users might have access to multiple health records. A HealthVault record can also be shared with software applications, devices and/or health organizations. This sharing creates trust relationships defined and controlled by the owner of the record. HealthVault provides programmer APIs and is compatible with sharing standards like SOAP, CCR/CCD and XML, enabling development of desktop and mobile applications.

III. Case Study

The primary challenge in e-Health is in the creation of a secure yet trustworthy environment that can facilitate sharing of not only health data but also associated information like access rights, meta-data, identities, trust relationships etc. This will allow patients to have full control of what entities, roles, or people can access their data. To understand what the problems are, we identify a number of use cases, which are difficult to accommodate using the current health care IT systems. In this section, we detail the scenario of a family that needs to care for one of its members, demonstrating the need to share health data, user identities and access rights across health domains. We also demonstrate strong governance, security and privacy.

A. *Grand scenario and actors*

A summary of the actors is presented in Table I. The first, and most important, actor is our care subject: *Deirdre Drake*, an elderly woman suffering from a chronic disease (COPD). *Deirdre* is very weak and housebound, but usually capable of living on her own. However, sometimes her condition deteriorates and she could be admitted to hospital. *Sam* and *Nigel Drake,* her sons, are determined to provide the best possible standard of living for their mother. *Sam* has a limited amount of time while *Nigel*, despite working primarily from home, he often needs to travel abroad for business. The two brothers have arranged for *Kate*, a registered nurse, to attend to *Deirdre* regularly and monitor her vital health signs. *Deirdre* is also monitored by *Mike*, a GP who periodically overviews her vital signs and other examinations. As a GP, *Mike* is registered with the health service. *Mike's* services are rarely needed, except when *Deirdre's* condition deteriorates. Should this happen, he needs to review the latest data in *Deirdre's* health record. To stage the use cases, we will hypothesize that *Deirdre's* condition deteriorates and she is admitted to hospital by *Nigel*. After being treated for a few days, *Deirdre* will return home, but will still be at high risk and in need of continuous medical attendance. This will be conducted by *Mike*.

B. *Use case scenarios*

The grand scenario allows us to identify two use cases, one demonstrating access rights sharing and one for health record sharing. Together, the use cases cover the complete patient pathway across the health domains. The following paragraphs briefly define our assumptions on the current

TABLE I. CASE STUDY ACTORS AND THEIR ROLE.

Actor	Role	Description
Deirdre	Patient	The care subject. Initially at home, then admitted to hospital and back home.
Sam	*Deirdre's* son	Custodian to *Deirdre's* HealthVault record.
Nigel	*Deirdre's* son	Creator (and custodian) of a HealthVault record for *Deirdre*
Kate	Nurse	*Deirdre's* nurse
Mike	GP	*Deirdre's* GP

non-computerized health system. Our solution for these scenarios on our e-Health system is discussed in Section IV.

1) *Trust sharing scenario*

Deirdre is admitted at the hospital, and *Nigel* calls *Sam*, to inform him about the situation. *Sam* is anxious about his mother but cannot leave work to visit her immediately. Family members of patients have no means to check how their relatives are doing, unless they visit the hospital. Technology should ease this frustrating situation by allowing relatives to view a patient's status, as long as the patient consents, emulating a real-life hospital visit.

2) *Data sharing scenario*

When *Deirdre* leaves the hospital, results undertaken examinations would be given to her as part of the dismissal process. This physical record would have to be included in a folder with other health data and then taken to the doctors who attend *Deirdre* regularly, i.e. *Mike*. Further updates to this record, i.e. additional data created by *Kate* when *Deirdre* returns home, would also have to be delivered to *Mike*. This transferring of a physical patient record from the hospital to informal care is a serious inefficiency of the current health system, which needs to be addressed.

IV. SYSTEM DESIGN

A. *Integrating the subsystems*

The integrated system is illustrated and paralleled with the health system in Figure 2. In the health system level, the health domains are illustrated along with patient transition between them. The e-Health level illustrates our system residing in the cloud. In order to enhance functionality and usefulness, we need to integrate DACAR and HealthVault in a way that preserves security policies and trust relationships pre-existing in both. The user must thus be able to: (a) access data and services in both subsystems, as long as they have an account in either of them; (b) replicate access rights and trust relationships between subsystems; and (c) replicate health record data between the subsystems. To facilitate this, we introduce an integration mechanism, a *Translation Gateway (TG)*, which allows for the translation of rights between the two subsystems and using a secure and trusted connection between them to facilitate the exchange of data. Ultimately, the *TG* is the component that integrates the subsystems into a single larger system. The *TG* itself consists of subcomponents dedicated to functionalities accommodating the case study. It will provide a web interface allowing execution of the possible tasks from a single web site.

B. *Trust sharing use case*

This case demonstrates the need to discover trust relationships pre-defined in HealthVault and replicate them into DACAR, allowing HealthVault users to access patient records controlled by DACAR. We will assume that *the Drake* brothers have already created and shared *Deirdre's* HealthVault record. *Nigel* will initially need to log in to the *TG* and authorize it to view *Deirdre's* record in HealthVault. This enables the *TG* to discover that *Nigel* is indeed a custodian of *Deirdre* and to store the gathered information in a mapping table, an example of which is provided in Table II. *Sam* will also need to authorize the *TG*, and let it discover his custodian access to *Deirdre's* record and similarly store the information in the mapping table. At this stage, the *TG* can match HealthVault user IDs using HealthVault record IDs as the matching key and confirm whether the brothers are custodians of the same record. Upon satisfying this condition, the *TG* will configure DACAR's SPoC to assign *Sam* with the same access rights as *Nigel*, equaling the HealthVault trust relationship. *Sam* is therefore allowed to access the EWS service from his workplace, despite this service residing in DACAR, for which he does not have an account.

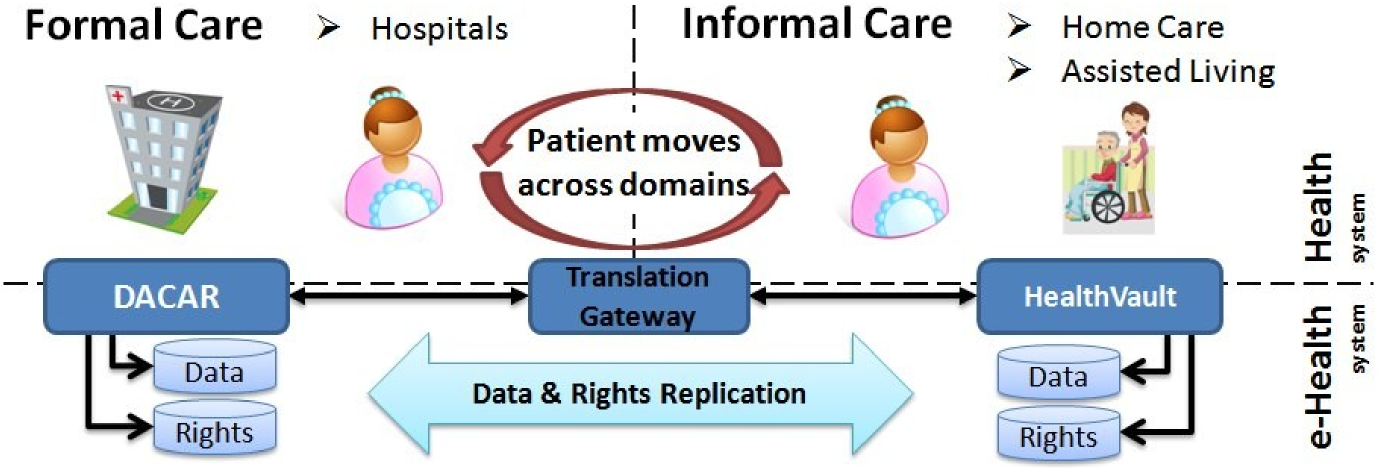

Figure 2: High-level overview of the system and its use.

TABLE II. THE MAPPING TABLE OF THE TRANSLATION GATEWAY.

Actor	DACAR user ID	HV ID	Own HV record ID	Custodian of HV record ID
Deirdre	-	-	1835	-
Nigel	3478	3494	-	1835
Sam	-	2948	-	1835

HV abbreviates "HealthVault"

C. Data sharing use case

This case demonstrates a key functionality enabling transition between formal and informal care. When patients visit hospitals, clinicians working there will need to access historical and recent patient data, regardless of where these have been generated. When patients leave the hospital, they need to allow informal carers to access and update data generated and stored while they were there. This case uses HealthVault for informal care data generation and DACAR for formal care data access, and then translates rights between the two depending if the patient is in a formal care setting (such as in a hospital), or an informal one (such as Assisted Living).

The *TG* is initially used as a data transfer tool, aiming to retrieve data from DACAR and upload it to HealthVault; when *Deirdre* leaves the hospital, *Nigel* will log in to the *TG* and will select the transfer action. He will be asked by HealthVault to authorize the *TG* for permanent (*offline access*) to the HealthVault record of *Deirdre* and thereafter, the *TG* can transfer all *Deirdre's* data held in DACAR into HealthVault. For demonstrative purposes, we will assume that at this point data is erased from DACAR. Later on at home, *Kate* measures and uploads *Deirdre's* blood pressure to HealthVault every day, using a HealthVault-compatible device, in order to allow *Mike*, the GP, to continue monitoring *Deirdre* after her hospitalization.

Then the role of the *TG* changes to a tool for managing authorization and retrieval of data to formal carers. Although *Deirdre's* data are not held in DACAR anymore and despite *Mike* not having a HealthVault account, the *TG* retains the permanent access to *Deirdre's* record in DACAR. This right can be utilized to allow formal carers to view their patient's data stored in HealthVault, by authorizing and authenticating themselves against DACAR only. *Mike* can log in to the *TG* and request an up to date copy of *Deirdre's* data. The *TG* will interface with the SPoC to confirm *Mike's* membership in the ROLE.GP group and that he is the GP of *Deirdre* in particular. If the conditions are satisfied, the *TG* will retrieve *Deirdre's* data from HealthVault and present them to *Mike*. Although the *TG* itself will have unrestricted access to the HealthVault record, the dissemination of data to non-HealthVault users will be controlled by DACAR's access control mechanism (the SPoC). Finally, the patient can remove the permanent access of the *TG* at their discretion.

V. SYSTEM EVALUATION

A. Security and privacy in the cloud

Our system demonstrates strong security characteristics, as it is made by securely integrating subsystems, which are providing strong security and privacy in their own right. The security of HealthVault is considered by Microsoft to be similar or stronger than what is required by HIPAA [21]. On the other hand, the security of DACAR follows good practices like database-level encryption, Kerberos authentication [20] and use of cryptographic signatures. Therefore, our challenge is to integrate them in a manner that will not compromise their security. This can be achieved by understanding their design and rationale behind their security requirements and behavior. Since all the subsystems have been developed within our consortium, we were well positioned to achieve these goals. Overall, we are confident that we can provide higher than average security and privacy levels and that our design demonstrates how to benefit from the advantages of the cloud without compromising security.

HealthVault is hosted on the Windows Azure Platform public cloud and it is therefore potentially vulnerable to typical public cloud -related security issues. These have been addressed very well by Microsoft, using database-level encryption and many other security and obscurity features. On the other hand, DACAR will most likely be deployed in a private cloud infrastructure and it therefore should be secure enough with a correctly implemented database-level encryption. However, DACAR can also operate on a hybrid cloud deployment scenario, as it supports application-level encryption as well. In such case, the data bucket server is deployed in the public cloud, exploiting availability, scalability and cost-efficiency, while the SPoC server remains hosted in a private cloud, managing the application-level encryption, including key distribution and storing.

The *Translation Gateway (TG)* minimizes weak links and treats all system components as non-trusted by default, making a security checks before any action. An important security feature used by the *TG* is the provided way to set up a secure communication channel with HealthVault, using PKI and digital signatures appropriately. The issue of privacy is addressed by the combination of governance features made available by the subsystems and by the *TG*, which only acts upon instruction by the patient. The patient controls whom or what can access their records and the kind of access they may have. Further restrictions imposed by the formal policies of the health service and local law are also enforceable by the subsystems.

B. Benefits to the patient

The system enables the patients to generate and share health data on seemingly different health domains. For example, data generated at home, prior to hospitalization, become available to doctors at the hospital in case of an emergency. Generating data at home, using HealthVault device ecosystem can decrease the cost of informal care. In our examples, that ability could help the brothers use an automated sensor network to monitor *Deirdre* constantly, even when *Nigel* is abroad. Furthermore, the sharing abilities enable patients to "carry" their health record electronically, instead of using time-consuming and difficult processes, like carrying physical copies of examinations to various consultants, GPs, pharmacies and so on, as the patient's record is available globally. The sharing ability is also very useful for patients who frequently travel between health systems, e.g. pensioners who buy retirement property abroad.

C. Benefits to health system

Utilizing cloud computing should allow the health system to benefit from economies of scale and higher availability. The data sharing abilities can improve the quality of care by empowering carers and allowing them to have access to a complete record of a patient's history and data generated across domains. The utilization of a *TG* can also solve compatibility with legacy systems, as it may translate data and let them be used in otherwise incompatible services and medical devices.

VI. Conclusion and Future Work

A. Conclusion

We believe that the failures of modern e-Health care can be avoided by using trustworthy systems designed with security and privacy in mind and by increasing awareness about the potential of these systems. This research presents such a system, integrating two subsystems originally meant to operate in different health care domains. Our solution enables a greater degree of patient record and identity sharing, provides strong security and privacy characteristics and is entirely governed by the patient, making it truly patient-centric. The system integrates an EHR system (DACAR) with a PHR system (Microsoft HealthVault) on a cloud-based infrastructure, blending e-Health models with cloud computing without compromising security, ease of use and cost efficiency. To evaluate our system, we have developed a case study narrating real world problems faced by patients, ultimately helping to overcome skepticism about the use of cloud computing in e-Health. Our solution provides a number of benefits to the patient and the health service. The patients are enabled to manage and share their health record health domains while the health service could provide cost-efficient, high-quality care.

B. Future work

At present, the *TG* is an early stage prototype. In the near future, we plan to finalize it in order to test it, firstly with the Patient Simulator [22] developed at ENU and then in real world clinical trial. This endeavor will include deployment in a UK hospital, and we will provide services to allow testing. We have also partner with Flexiant, a UK-based independent cloud provider, in order to host the DACAR subsystem for development, testing and clinical trials. We will also embark in an awareness campaign to improve human trust in e-Health systems, primarily targeting health officials and doctors. Later stages of the project will include integration of more identity management systems, like U-Prove [23] as well as compliance with Continua Health Alliance standards.

References

[1] Greenhalgh, T., et al., *Adoption and non-adoption of a shared electronic summary record in England: a mixed-method case study.* BMJ, 2010. **340**(jun16_4): p. c3111+.

[2] Wainer, J., et al., *Security Requirements for a Lifelong Electronic Health Record System: An Opinion.* Open Med Inform Journal, 2008. **2**: p. 160-165.

[3] Barr, F. *GPs back cuts to NHS Direct and NPfIT.* eHealth Insider [Blog news article] 2010 [cited 2011 12/05/2011]; http://www.ehi.co.uk/news/primary-care/5668.

[4] Bruce, S. *NPfIT failures have left NHS IT "stuck".* eHealth Insider [Blog news article] 2011 [cited 2011 12/05/2011]; http://bit.ly/qgE69u.

[5] *ISO Technical Committee 215, Health Informatics.* 2011.

[6] *Health Level Seven International (HL7)*. 2011.

[7] *Data Protection Act*. 1998: UK. http://bit.ly/qklddI.

[8] *Health Insurance Portability and Accountability Act (HIPAA)*, U.S. Congress. 1996. http://1.usa.gov/djyKE.

[9] Fan, L., et al. *DACAR Platform for eHealth Services Cloud.* in *IEEE Cloud 2011*. 2100.

[10] Lorence, D., et al., *Toward a patient centric medical information model: issues and challenges for US adoption.* International Journal of Electronic Healthcare, 2005. **1**(4): p. 349-364.

[11] Sunyaev, A., et al., *Evaluation Framework for Personal Health Records: Microsoft HealthVault Vs. Google Health.* Hawaii International Conference on System Sciences, 2010. **0**: p. 1-10.

[12] Wartena, F., et al. *Continua: The Impact of a Personal Telehealth Ecosystem*. in *International Conference on eHealth, Telemedicine, and Social Medicine, 2009. eTELEMED '09.* 2009.

[13] Kilic, O., et al., *Providing Interoperability of eHealth Communities Through Peer-to-Peer Networks.* IEEE TITB, 2010. **14**(3): p. 846-853.

[14] Jha, A., et al., *Use of Electronic Health Records in U.S. Hospitals.* The New England Journal of Medicine, 2009(360): p. 1628-1638.

[15] Caldwell, T. (2011) *Two hospitals share a hosted private cloud*. SearchNetworking. http://bit.ly/gax8Ya.

[16] Sunyaev, A., et al. *Open Security Issues in German Healthcare Telematics*. in *Proceedings of the Third International Conference on Health Informatics (HealthInf 2010)*. 2010. Valencia, Spain.

[17] *Gematik - Gesellschaft Telematikanwendungen der Gesundheitskarte*. 2011; http://www.gematik.de.

[18] Nguyen, A. (2010) *Hospitals reduce IT support hours with remote desktop management*. COMPUTERWORLDUK. http://bit.ly/qhEwzl.

[19] *Kodit: CAREMagic*. 2011; http://www.kodit.com/markets/caremagic/.

[20] Tung, B., *Kerberos: a Network Authentication System*. 1999, Addison-Wesley: Reading, MA.

[21] Microsoft (2009) *Microsoft HealthVault and HIPAA*.

[22] Lo, O., et al., *Patient Simulator: Towards Testing and Validation.*, in *Pervasive Health 2011*. 2011: Dublin.

[23] Microsoft. *Microsoft U-Prove Community Technology Preview R2.* 2011 [cited 2011 12/05/2011]; http://connect.microsoft.com/site1188.