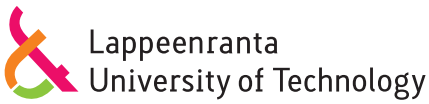



Were Oyomno

# USABLE PRIVACY PRESERVATION IN MOBILE ELECTRONIC PERSONALITY

Thesis for the degree of Doctor of Science (Technology) to be presented with due permission for public examination and criticism in the Auditorium 1382 at Lappeenranta University of Technology, Lappeenranta, Finland on the 24th of August, 2012, at noon.

Acta Universitatis
Lappeenrantaensis **479**

Supervisors Professor Jari Porras
Laboratory of Communications Software
Department of Information Technology
Faculty of Technology Management
Lappeenranta University of Technology
Finland

Dr. Tech. Pekka Jäppinen
Laboratory of Communications Software
Department of Information Technology
Faculty of Technology Management
Lappeenranta University of Technology
Finland

Reviewers Professor Tuomas Aura
Department of Computer Science and Engineering
Aalto University
Finland

Professor Denis Trček
Laboratory of e-media
Faculty of Computer and Information Science
University of Ljubljana
Slovenia

Opponent Professor Josef Noll
Department of Informatics
Networks and Distributed Systems
University of Oslo
Norway

ISBN 978-952-265-266-9
ISBN 978-952-265-267-6 (PDF)
ISSN 1456-4491

Lappeenrannan teknillinen yliopisto
Digipaino 2012

## Preface

The research work reported in this thesis was carried out in the Laboratory of Communications Engineering in the Faculty of Technology Management of Lappeenranta University of Technology, Finland, during the years 2009 - 2012. The completion of this work could not have been possible without the invaluable assistance and support I received from many people, including my supervisors and colleagues at the University, my friends in Finland, South Africa and most of all the members of families. Because the list is too long to fit in the limited space available, I am unable to include all your names here. Nevertheless, take note of my deep appreciation of your support as I humbly acknowledge here.

Having said that, this acknowledgement would not be complete without a mention of a few names. My very special thanks go to my supervisors Prof. Jari Porras, Prof. Esa Kerttula and Pekka Jäppinen for their belief in my ability to undertake challenge, and the many long hours spent going through the motions of researching: conceptualising, modelling, experimenting, discussing and reviewing various aspects of the work. Gentlemen, you kept me going especially when the going was so tough that despair seemed a more attractive option. In the same token and breath, I convey my gratitude to Kari Heikkinen for the invaluable discussions on usability issues, and Jouni Ikkonen for the conducive research environment, and to my colleagues at the Communication Software Laboratory for maintaining an inspiring research atmosphere. I also wish to acknowledge with deep gratitude the invaluable contributions of my pre-examiners Prof. Denis Trček and Prof. Tuomas Aura. Your expertise, experience and intimate knowledge on the subject, and guidance were invaluable inputs to the the finalisation of the thesis.

Apart from the contributions and support from academic colleagues and friends, I would like to acknowledge the significant role my families played in providing me with a solid foundation on which to build and nurture a strong belief in and commitment to hard work. My special gratitude goes to my parents, Violet and Gordon Oyomno and Merja and Hekki Karhunen for the wisdom, encouragement and advice especially when those were needed most. Last but not least, I am truly grateful to my loving Veera for her love, patience, understanding and above all, being ever supportive. Veera, I owe you much more than this, and you know it!

Lappeenranta, August 2012

*Were Oyomno*

## Abstract

Were Oyomno
**Usable Privacy Preservation in Mobile Electronic Personality**
Lappeenranta, 2012
106 p.

Acta Universitatis Lappeenrantaensis 479
Diss. Lappeenranta University of Technology

ISBN 978-952-265-266-9
ISBN 978-952-265-267-6 (PDF)
ISSN 1456-4491

Personalised ubiquitous services have rapidly proliferated due technological advancements in sensing, ubiquitous and mobile computing. Evolving societal trends, business and the economic potential of Personal Information (PI) have overlapped the service niches. At the same time, the societal thirst for more personalised services has increased and are met by soliciting deeper and more privacy invasive PI from customers. Consequentially, reinforcing traditional privacy challenges and unearthed new risks that render classical safeguards ineffective. The absence of solutions to criticise personalised ubiquitous services from privacy perspectives, aggravates the situation.

This thesis presents a solution permitting users' PI, stored in their mobile terminals to be disclosed to services in privacy preserving manner for personalisation needs. The approach termed, Mobile Electronic Personality Version 2 (ME2.0), is compared to alternative mechanisms. Within ME2.0, PI handling vulnerabilities of ubiquitous services are identified and sensitised on their practices and privacy implications. Vulnerability where PI may leak through covert solicits, excessive acquisitions and legitimate data re-purposing to erode users privacy are also considered.

In this thesis, the design, components, internal structures, architectures, scenarios and evaluations of ME2.0 are detailed. The design addresses implications and challenges leveraged by mobile terminals. ME2.0 components and internal structures discusses the functions related to how PI pieces are stored and handled by terminals and services. The architecture focusses on different components and their exchanges with services. Scenarios where ME2.0 is used are presented from different environment views, before evaluating for performance, privacy and usability.

Keywords: Ubiquitous Computing, Context-awareness, Privacy, Personalisation

UDC 004.5:004.89:004.031.6:621.39

| | |
|---|---|
| 3G | Third Generation Mobile Telecommunications |
| AA | Authorisation Authority |
| AC | Authorisation Certificate |
| AP | Access Point |
| ATRACO | Adaptive and Trusted Ambient eCOlogies |
| *bdaddr* | Bluetooth Device Address |
| CA | Certificate Issuing Authority |
| CBF | Content Based Filtering |
| CF | Collaborative Filtering |
| CIA | Confidentiality, Integrity and Authenticity |
| CnP | Context-Notated Preferences |
| CoP | Content Provider |
| CP-net | Conditional Preference network |
| CPU | Central Processing Unit |
| DoB | Date of Birth |
| DoS | Denial of Service |
| EA | Enforcer Authority |
| ECC | Elliptic Curve Cryptography |
| ECDH | Elliptic Curve Diffie-Hellman |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| ECML | Electronic Commerce Modelling Language |
| EPAL | Enterprise Privacy Authorisation Language |
| GPS | Global Positioning System |
| HCM | Hybrid Context Model |
| HTTPS | Hypertext Transfer Protocol Secure |
| ID | Identity |
| IM | Instant Messaging |
| IPv6 | Internet Protocol version 6 |
| IT | Information Technology |
| ME | Mobile Electronic Personality |
| ME2.0 | Mobile Electronic Personality Version 2 |
| ME2ML | ME2.0 Modelling Language |
| NP/GII | Non-Personal or Group Identifiable Information |

| | |
|---|---|
| OBEX | Object Exchange |
| OBM | Ontology Based Model |
| ORM | Object-Role Model |
| P/GPref | Personal or Group Preference |
| P/GII | Personal or Group Identifiable Information |
| P3P | Platform for Privacy Preferences |
| PC | Personal Computer |
| PI | Personal Information |
| PII | Personal Identifiable Information |
| PIN | Personal Identification Number |
| PKI | Public-Key Infrastructure |
| PRS | Personal Remote Server |
| PSN | PlayStation Network |
| PzI | Personalisation Information |
| RAM | Random Access Memory |
| RFCOMM | Radio Frequency Communications |
| RFID | Radio Frequency Identifier |
| S/CI | Situation or Context Information |
| SAA | Service Accessing Application |
| SAD | Service Accessing Device |
| SAML | Security Assertion Mark-up Language |
| SDSI | Simple Distributed Security Infrastructure |
| SI | Sensitive Information |
| SIM | Subscriber Identity Module |
| SMS | Short Message Service |
| SN | Social Networking |
| SPKI | Simple Public-Key Infrastructure |
| SQL | Structured Query Language |
| SSN | Social Security Number |
| TTP | Trusted Third Parties |
| XACML | eXtensible Access Control Mark-up Language |
| XML | Extensible Mark-up Language |
| ubicomp | Ubiquitous Computing |
| UI | User Interface |
| Wi-Fi | Wireless Fidelity |
| WLAN | Wireless Local Area Network |
| WWW | World Wide Web |

Chapter I

# Introduction

## 1.1 Privacy within personalised services

In today's world, average consumers often find themselves bombarded with vast amounts of information from various sources, of varying quality and at different time intervals. The bombardments are through diverse information channels such as E-mails, billboards, television, radio, Social Networking (SN) and telephones. The resulting *"information overload"* [7] to which consumers are exposed constrains their ability to make reasonable assessments and judgements of the situation and the best causes of action at their disposal. Numerous factors contributing to and accounting for the overload include the increased rates at which new information is produced, the ease of creating, duplicating and transmitting the information, the expansions of bandwidths and the creation of entirely new channels for transmitting the information, the expansions of bandwidths and the creation of entirely new channels for transmitting all forms of multimedia information.

The ability of consumers to filter out irrelevant content from the vast information would improve their ability to make reasonable decisions and correct assessments of their information needs. Information filtering on the basis of a consumer individuality and preference is termed personalisation. In personalising information, consumers are presented with a balance of relevant and useful content from appropriate channels at appropriate times.

Personalisation may also be extended to generic services by focussing them to appeal to a specific user needs, such as reducing the efforts they require to accomplish certain tasks. *Airline ticketing service*, *ubiquitous information screens* and *meal locators* are examples of services that users can advantageously personalise. The airline ticketing service aids users in the reservation and purchasing of airline tickets using Internet-connected terminals. While the information screen adapts its content to display those relevant to the users, the meal locator eases efforts made when locating appropriate restaurants serving the user's preferred meals.

Individuals have dynamic preferences that change frequently even while accessing per-

sonalised services. For example, while not all individuals prefer or are willing to purchase and fly business class, their preference or willingness is likely to change in cases of emergency or free offer. Another relevant scenario is adapted from the 2002 film, *Minority Report* [140]. In the train station scene of the film, the character John Anderton a rogue law enforcer, is pursued by fellow law enforcers. John expects to go unnoticed in the densely populated station, but unfortunately personalised information screens at station fail to note the change in his preference. The screens identify and single out John for personalised advertisements alerting his pursuers of his location.

In this regard, the suitability or credibility of a *one-size-fits-all* principle, that provides all users with identical services, information, meals and treatments, irrespective of their preferences, situations or individuality is questionable. Providing generic services would most likely lead to wastage of time and resources and mismatched preferences resulting in user frustration and dissatisfaction. As a strategy, personalising services to a user preferences seeks to address the weaknesses of generic service offerings.

In order to personalise offered services, service providers require some information from potential users. The information required includes users Personal Information (PI) (such as their names, age or gender), preferences (such as favourite film, favourite music, disliked beverage) and contextual settings (such as current activity, accompaniment, location), as Figure 1.1 depicts. Identifiable information is one of the main categories of PI required by services as shown in Figure 1.1. Identifiable information or "strong identifiers" serves the important role of acting as a marker for other PI to uniquely identify an individual. It is therefore not exclusively required for personalisation purposes. There also exist "weak identifiers" in PI such as gender and age that may identify a group of individuals. When multiple weak identifiers are used in combination, they may distinguish a single individual. Furthermore, the nature of identifiers may be weak or strong depending on situation of their use. This study excludes identifiable information or strong identifiers from Personalisation Information (PzI) category and attempts to minimise the direct usage and combinations of weak identifiers for personalisation. Figure 1.1 is by no means an exhaustive account of all PzI. Rather, it is an attempt to characterise the primary PzI excluding secondary attributes derived of aggregates and recorded history.

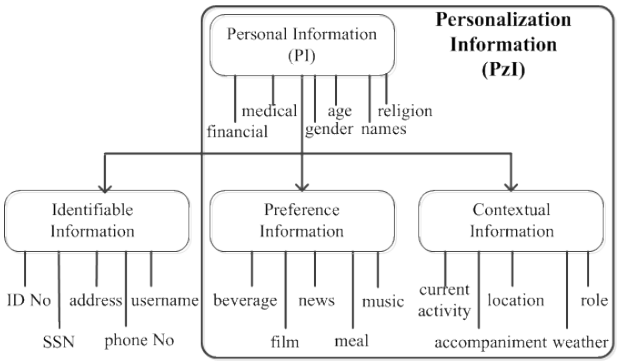



**Figure 1.1:** PzI.

The nature and amount of PI services solicit from users depends on the character of service and its intended level of personalisation. For example, the airline ticketing service

mandates PI of the user's passport details, travel schedules and payment credentials to *facilitate* the flight service. However, the meal locator service obligates PI pieces such as the user's current location, food allergies, budget, dietary preferences and arrival time, to *enhance* its restaurant listing service. Notably, PI required to facilitate a service are often more personally identifiable compared with that required for service enhancement.

A service providers that innovatively uses consumers' PzI to provide a uniquely individualised user experience that appeal to the customers and differentiates them from their competitors are likely to have a competitive advantage over their competitors.

Within the last decade, numerous personalised services have emerged and existing ones evolved, others have transformed and matured. Today, Internet based services such as Amazon [9], e-Bay [38] and Google [55] offer highly personalised services to customers. Amazon for example, aggregates its consumers behaviour and history of browsing, purchases and wish lists, to personalise its offers to other customers under appealing titles such as *"today's recommendations for you", "frequently bought together", "customers who bought item X also bought item Y", "most wished for in films and television"* and *"what other customers are looking at right now"*.

Different personalised services have also been merged to extend seamlessly the reach and appeal of their personalised offers to customers. Techniques adopted by services to solicit, collect and store PzI from their customers have been transformed in order to enable implicit and transparent retrievals from heterogeneous terminals. These transformations have extended the applicability of personalisation techniques to the off-line environments of users and their terminals.

Terminals that users use to access personalised services have also been miniaturised, mobilised and detached from the constraints of their stationary predecessors like desktops and workstations. The detachment has two implications. Firstly, users now access services from anywhere, any-time, while mobile and under constantly changing situations using their mobile terminals. Secondly, PzI stored or sensed by the mobile terminals can be used to personalise services accessed by users.

The maturity of personalised ubiquitous services is largely attributed to technological advancements in mobile computing, ubiquitous infrastructures and sensing technologies. Within the last five years, the processing capacities of mobile terminals have more than quadrupled. Comparisons of the 332MHz Central Processing Unit (CPU) of a 2006 Nokia N95 with a 2011 Nokia Lumia 800's 1.4GHz or Samsung I9100 Galaxy SII dual-core 1.2GHz CPU drives the point home [112, 134]. The Random Access Memory (RAM) and storage capacities of these terminals have also increased in the same period. For example, compare the RAM and storage capacities of Nokia N95 (64MB and 8GB) with that of Samsung I9100 Galaxy SII (1GB and 64GB). Similarly, network bandwidths and data rates have more than doubled in the terminals as is evident in Wireless Local Area Network (WLAN) from 802.11g (20MHz, 54Mbits/s) to 802.11n (40MHz, 150Mbit/s) and Bluetooth from 2.0 (2.1Mbits/s) to 3.0+HS (24Mbits/s) [68, 122, 132]. Various ubiquitous networking technologies such as Wireless Fidelity (Wi-Fi), Bluetooth [123], ZigBee [144] and Third Generation Mobile Telecommunications (3G) have been incorporated into mobile terminals. The terminals have also become smarter and more aware of their surrounding due to an array of in-built sensors such as accelerometers, Global Positioning System (GPS) receivers, proximity, gyroscope, orientation, audio and touch

sensors. The sensor technologies in mobile terminals have been simplified, made more energy efficient and affordable to suit different niche markets and interact with various wireless communication technologies. ZigBee for instance, is a wireless communication technology suitable for automation of lighting, heating, cooling and security in buildings and metering. Ultra-Wideband (UWB) [57, 153] is useful in sensor data collection, precision triangulations and tracking. The Internet Protocol version 6 (IPv6) over Low Power Personal Area Networks (6lowpan) [107] has made it possible to address sensors universally.

In addition and running parallel to these technological and service advancements, is the trend of lowering of barriers to the composition, development,distribution and deployment of services, thus making it increasing easier and faster. Learning curves for service composition tools like Integrated Development Environment (IDE), software development kits and Application Programming Interfaces (API) have been simplified making them easy to master and use. At the same time, service deployment and distribution channels such as the iPhone applications store, Nokia Store, Android market (re-branded to Google Play in 2012) and Windows Phone Marketplace are widely accessible [52]. The combination of lowered barriers and the marketing of services, coupled with useful and user friendly services account for the growing popularity of mobile terminals popular and their widespread at work and at home [51].

These trends have provided a mature platform upon which easily developed and deployed services can solicit deeper and richer PzI from users' mobile terminals to effectively personalise their offerings to individual preferences. Such efficacies have propagated personalised ubiquitous services into sectors of governance (E-governance [131], E-citizen [31]), business (E-commerce, M-commerce [94, 145]), healthcare (M-health [139]), community (virtual communities, M-learning, E-learning [146]) and domestic lives (assisted living [61, 23]). Natural extensions of these efficiencies anticipates further deepening of solicited PzI, their systematic storage and progressive distribution across the sectors to attain seamlessness, transparency, differentiations and societal efficacies.

In societies where individuals PzI are efficiently retrieved and delivered to services thereby depriving owners of their control, privacy is a growing concern. The concerns become more real as developers continue to ignore prioritising users' needs in their haste to market products [147]. In more ways than one, these societies resemble the Orwellian [115] society which advocated for constant surveillance of citizens by Big Brother using *"telescreen"* [115]. Deeper similarities emerge as the societies evolve and demand more PI for participation in social activities such as driving, shopping, healthcare and insurance. Further similarities exist in the amendments of legislations to permit stealth surveillance and covert solicitations in the interest of national security. For instance, post 9/11 the United States government amended the Homeland Security Act to consolidate federal agencies under a single umbrella and eliminating inter-agencies information firewalls. It also enacted the Patriot Act to allow these agencies to collect vast amount of surveillance information in their efforts to *"total information awareness"* [147]. Worldwide, legislative amendments of data protection of electronic communication are on the rise. In June 2008 the Swedish parliament passed law permitting their intelligence bureau to eavesdrop and conduct general surveillance on citizens' international calls, faxes and E-mails [46]. Five months later (November 2008), the Finnish parliament amended their data protection and electronic communications legislation commonly known as "Lex Nokia"

or the *snooping law*, to permit employers to investigate employees E-mail and Internet traffic logs on suspicion on leaked corporate secrets [64].

One testament to these concerns is the recent rise in the number of reported privacy compromises and their severity, which has further aggravated consumer anxiety. Recent compromises in the media has involved Facebook connected smart-phones [96], IPv6 enabled smart-phones [82, 154], Wal-Mart Radio Frequency Identifier (RFID) monitoring [129, 49], Fine Gael 4000 voter's compromise in Ireland [63] and Sony PlayStation Network (PSN). In the PSN incident of 25 April 2011, malicious entities compromised vital credentials of 77 million users. The credentials in question were names, Date of Birth (DoB), physical addresses, E-mail addresses, PSN/Qriocity passwords, logins, handles, on-line identity and credit card numbers [138]. There are also many more services that are reluctant to publicise their compromises for fear of tarnishing their reputations and any other negative repercussions.

Such privacy compromises demonstrate that reliance on services alone to guarantee user privacy is considerably inadequate and possibly misplaced and ignorant altogether. Yet, trends indicate that personalised services and thier facilitators continue to increase in numbers and sophistication [52]. The increase is attributed to the rise in number and intelligence of mobile terminals and their supporting infrastructures. Gartner research predicts that the top ten mobile arenas to significantly grow in the year 2012 will include Location Based Services (LBS), context-aware services, Object Recognition (OR), mobile search, SN, M-commerce, Mobile Instant Messaging (MIM), mobile E-mail and mobile video [51]. Unless key stakeholders give attention to consumer privacy, a considerable amount of funds may have to be spent on victims' compensation, privacy recovery and public reassurance.Therefore, mechanisms permitting access to personalised ubiquitous services without compromising user privacy are needed. This is the problem this study inquired into.

## 1.2 Research question

The main research question posed for the study was: **how can users obtain personalised ubiquitous services without compromising their privacy?** In resolving this question, sub-questions emerged.

First, to access personalised services, users must disclose portions of their PI. However, not all disclosed PI result in a privacy compromise. Determining the privacy invasive components permits the adoption of appropriate safeguards. The determination can be done by asking the question: *what PI items are privacy invasive and in what ways?*

After determining the privacy invasive PI items, other PI emerges which is usable for personalisation. Ensuring appropriate mechanisms to identify non-privacy invasive PI raises the question of: *how should PzI be separated from PI to preserve privacy?*

To be able to make privacy decision based on their PI, answers are required to the question: *How can users organise and manage their PI in a privacy preserving manners?*

As users disclose their PI to services for personalisation, they also surrender some control over safeguarding its privacy. In ensuring that privacy safeguards are retained, answers are required to the question: *How can users ensure that services handle/process their disclosed PI appropriately?*

## 1.3 Purpose and scope of research

The objectives of this research work were to identify and evaluate mechanisms permitting users to personalise and access ubiquitous services without excessive compromise of their privacy. The goal was to show different mechanisms that place considerably more control of PI with the users. The intention was to contrast alternative mechanisms as to their advantages and disadvantages, and justify this by utilising existing protocols with a few modifications, users can indeed personalise and access ubiquitous services in a privacy preserving manners. To this end prototypes and tests were implemented in the laboratory environment and the core concepts validated by real users in usability trials.

The thesis describes Mobile Electronic Personality Version 2, a mobile terminal application responsible for safely disclosing PzI to ubiquitous services. The disclosure of PzI pieces enables services to personalise their offerings to individuals' preferences. Preceding this thesis, is the Mobile Electronic Personality (ME) study [71]. The solution advocated by ME is for users to store their PI in their mobile terminal from where they may provide to services. This study and Mobile Electronic Personality Version 2 (ME2.0) extends ME by incorporating context-awareness, privacy awareness and usability studies. User perspective is dominant in ME2.0 and is highlighted in conducted usability studies.

This research was scoped to focus on the personalisation and access of ubiquitous services using PI items originating from ME2.0. These PI items are sourced from the in-built sensors of mobile terminals, terminal applications, planned activities, and the user's explicit input. Services with financial implications such as mobile terminal purchases are outside the scope of this study. The services considered in this study are accessed in a non-interactive manner or transparently, thereby differentiating them from Internet based services that are accessed interactively. This study also focuses on primary PzI as depicted in Figure 1.1 and considers higher level PzI such as historical and aggregate information out of scope as they would introduce further complications.

This study focuses on widely adopted ubiquitous networks that are easily available and have minimal cost implications. The proposals and implemented solutions are based on consumer-service provider interchanges over Bluetooth but can be easily replicated to other ubiquitous technologies such as WLAN and 3G.

## 1.4 Methodology

The methodology adopted for this study has three main parts as depicted in Figure 1.2 These parts are shown in the figure as shaded ovals and include: the conceptual-analytical research, the constructive research and the usability and artefact evaluation with prototyping. Illustrated in Järvinen's [73] taxonomy on research methods in Figure 1.2, the research work in this study has followed approaches to study reality. The conceptual analytical research critiques the status quo on privacy implications of personalised ubiquitous services. Stemming from this sensitisation are the challenges and limitations of existing personalised context-aware services in leaking users' PI.

The constructive research, denoted by the rectangle named "artefact building approaches" in Figure 1.2, leads to the development and implementation of ME2.0 to mitigate these challenges and limitations. Subsequently, the ME2.0 implementation is evaluated by

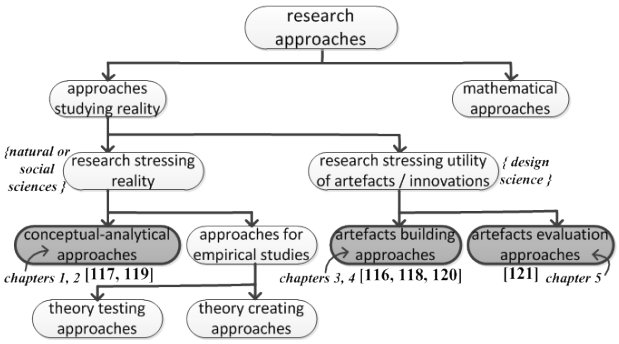



**Figure 1.2:** Taxonomy of research methods [73].

conducting usability testing with users. The ME2.0 architecture is also evaluated using case studies and prototypes.

## 1.5 Contributions of the research

The research reported has made significant contribution in three main ways in the areas of personalising ubiquitous services and privacy. Firstly, the considerations of existing ubiquitous services reveal privacy implications, challenges and limitations that threaten to compromise users' PI in the transfer of PzI. These implications are critiqued and addressed in [117, 119] which directly contribute towards the concept of notating PI with context. This contribution coincides with the left-most shaded oval in Figure 1.2.

The second significant contribution relates to the formulation, standardisation and implementation of service providers handling practices that are transparently presented in users' mobile terminals allowing for implicit privacy decisions based on a user's privacy expectations discussed in [116, 118, 120]. Additionally, the existence of a Trusted Third Parties (TTP) Enforcer Authority (EA) guarantees that solicited PzI are handled as stipulated in service providers' policies. This contribution along with safeguarding the information screen scenario are depicted in Figure 1.2 middle shaded oval.

Thirdly, by placing all the studied components into a common framework, the need for personalisation and access of ubiquitous services to be user centric is emphasised in [121] and the right most shaded oval in Figure 1.2. The focus on user perspective reduces the amount of effort required to manage privacy preferences and expectations, so that disclosures with services are not privacy excessive. This is all achieved without the knowledge of the underlying technologies and cryptographic suites. The results demonstrate that users can personalise local and external ubiquitous services without compromising or losing privacy altogether.

## 1.6 Thesis outline

This thesis is divided into six chapters. Chapter 2 sensitises the privacy challenges and implications of context, preferences and PI in personalising ubiquitous services. Different

mitigation strategies for these challenges are also presented and evaluated. In Chapter 3, ME2.0 is presented. This presentation begins with the architecture and then expands on how different artefacts are orchestrated to control and safeguard PI disclosures. Chapter 4 discusses ME2.0 usage scenarios with different services. An evaluation of ME2.0 from usability, performance and privacy perspectives is presented in Chapter 5. Chapter 6 concludes this study by providing the future research directions and conclusions.

## 1.7 Author's publications

Despite structuring this dissertation manuscript in a monograph format, the conceptual-analysis, the artefact building and artefact evaluation stages of the study depicted in Figure 1.2 have been conducted and the results published in the listed peer-reviewed articles. The referenced publications [117, 119, 116, 118, 120, 121] contribution to the study have been summarised in Section 1.5 and throughout the manuscript where deemed necessary.

- [117] W. Oyomno, P. Jäppinen and E. Kerttula, "Privacy Implications of Context-Aware services", in *Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middlewaRE (COMSWARE 2009)*, Dublin, Ireland. June 2009.
- [119] W. Oyomno and P. Jäppinen and E. Kerttula, "Privacy Preserving Architecture for Context-Enhanced Personalised Pervasive Screens", in *proceedings of Pervasive Computing Workshop on pervasive advertising and shopping (Pervasive2010)*, Helsinki, Finland. May 2010.
- [116] W. Oyomno and P. Jäppinen, "Security and Privacy in a Ubiquitous Information Screen", in *Proceedings of the 7th Minema Workshop (WAWC08 conference)*, Lappeenranta, Finland. August 2008.
- [118] W. Oyomno, P. Jäppinen and E. Kerttula, "Privacy Policy Enforcement for Ambient Ubiquitous Services", in *Proceedings of the First Joint Conference on Ambient Intelligence (Ami-10)*, Malaga, Spain. November 2010.
- [120] W. Oyomno, P. Jäppinen and E. Kerttula, "Privacy Preservation for Personalised Services in Smart Spaces", in *Proceedings of the Baltic Conference on Future Internet Communications (BCFIC2011)*, Riga, Latvia. February 2011.
- [121] W. Oyomno, P. Jäppinen, E. Kerttula and K. Heikkinen, "Usability study of ME2.0 - User Interface Design for Mobile Context Enhanced Personalisation Software", in *Proceedings of the Journal of Personal Ubiquitous Computing*, Springer London, UK. October 2011.

Chapter II

# Personal Information and privacy

Mobile terminals in use today store information from various sources of varying qualities and frequencies. The volume and complexity of the stored information often overwhelm users especially when they lack clear organisation structures required to discern its appropriate use. While such information could be used to personalise services, the danger is that such PI could become easily accessible to other persons to the detriment of individual owners. This thesis aims to use the information to personalise services without leaking the owners PI. It is therefore in the best interests of users that the information is organised in a manner that supports service personalisation and ensures privacy preservation.

The part of the stored information is the individual's PI that has different characteristics and is suitable for different uses. For example, identifiable information that is parts of the PI change less frequently than context or preference information. While context and preference information are less significant in personalisation, it is needed to establish associations and service facilitation.

When users disclose parts of their PI suitable for personalisation (PzI) to services, they receive personalised services. To receive differently personalised services, users disclose different parts and quantities of their PI. Travellers disclose their passport details such as names, DoB and nationality to the airline service to reserve seats. For the meal locator passport details have less importance in comparison to the current location and preferred meal. Disclosing PI serves the conflicting interests of users and services. For users, PI disclosures grant them services personalised to their individuality that are convenient and easy to use. For services disclosures are means to align and adapt their offerings to their customer preferences potentially resulting in higher satisfaction, loyalty and revenues [89]. In the conflict, users aim to minimise disclosures of their PI while services attempt to maximise PI solicitations to better understand their customers, increase the likelihood of present and future revenues.

## 2.1 Personal Information

Determination of which items of the PI stored in users' mobile terminals are important in making the right privacy decisions on their disclosure is a key concern in the development of service personalisation capabilities of mobile terminal technology. Differences in the constituents of PI spans the domains of users, academia, corporations and governments. Understanding PI in mobile terminals creates clarity and better understanding of privacy implications of interacting with services across these domains.

In defining PI and what it encompasses, users' perspectives tend to be subjective. Different users will include and exclude different information items. They will also modify and update these inclusions and exclusions overtime for different reasons and in different situations. One user might consider his E-mail address to be public information and freely disclose it, while another user will duly safeguard his E-mail address disclosures in different situations. This user subjectivity of PI is a motivation for governments to take steps to objectively define PI for their citizens. Objectivity minimises any misunderstandings of stakeholder disclosure, requesting and handling of PI.

The European Union Data Protection Directive 95/46/EC [45] defines PI for the citizens of its member states under the term *"personal data"*. Within the European Union context, personal data encompasses *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity;"* [45]. The United States government adopts the term *"Personal Identifiable Information (PII)"* and considers PI as any *"information which can be used to distinguish or trace an individual's identity, such as their names, Social Security Number (SSN), biometric records, etc. alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."* [109].

In academic literature, PI definitions are mostly from Personal Information Management (PIM) perspectives. Scholars such as Erickson [43], Heikkinen et al. [74], Al-Fedaghi [3] and Civan et al. [30] share this perspective. Erickson for instance, considers PI as *"any information that is owned by a person, such as a calendar, maps, notes, addresses etc."*. Discussions on inclusions of user requirements, user actions, context-awareness and conformity information to Erickson's definition of PI are raised by Heikkinen et al. [74]. Al-Fedaghi and Civan et al. highlight the ambiguity associated with the inclusions in and exclusions of various information items from PI. To address this ambiguity, scholars have divided PI into subsets based on their identity, their sensitivity and their privacy [3, 30].

Arguably, different interpretations and definitions of PI emerge depending on the perspectives adopted, the law of the land and the interests at stake. This study takes the user's perspective and their interests in regulating disclosures of their PI. Therefore, in the context of this thesis PI is similar to any *information individually or collectively generated or that is owned by a user.* From this definition it follows that PI encompasses *"any individual's or group's identifiable information, physical or electronic, including their names, addresses, phone numbers, race or ethnicity, nationality, origin, religious*

*or political affiliations, age, gender, sexual orientations, marital/family status, identifiable numbers, codes, symbols, registers, biological (fingerprints, blood types, inherited traits, medical records or history), educational, financial, criminal, employment records, opinions, personal views, preferences, and situational information that can be used to dissociate them from the population."* Stemming from the perspectives taken by this thesis and Al-Fedaghi works [3, 4] PI is sub-divided as Table 2.1 depicts.

**Table 2.1:** Sub-divisions, definition and instances of PI

| Terms | Definition | Instances or examples |
|---|---|---|
| Personal or Group Identifiable Information (P/GII) | PI distinguishing user(s) from the population allowing them to be uniquely identified, contacted, or located | SSN, identity number, uncommon names, passport details, registers, credit card details, DoB, birthplace |
| Non-Personal or Group Identifiable Information (NP/GII) | PI less distinguishing user(s) as they are common to members in a population, or a population group. They combine with other PI to make them P/GII | Common names, country, postcodes, city, age, gender, ethnicity, workplace, grades, titles, records |
| Sensitive Information (SI) | Users' privileged PI with potential of causing harm/loss if compromised | Medical, financial, religious, and political details their records or status |
| Situation or Context Information (S/CI) | Settings within which user(s) activity/event occurs | At work, at home, during lunch break, on holiday, humid, hot, tired. |
| Personal or Group Preference (P/G-Pref) | PI associated with likes/dislikes to customise experiences or expectations | Preferred language, music, films, meals, and restaurant. |
| Contactable information | PI enabling users to be contacted, communicated or interacted with | Work/home address, E-mail, Instant Messaging (IM), phone/fax numbers. |

Individuals' unique attributes that sufficiently distinguish them from the population and permit their accurate isolation in order to identify, contact, or locate them are PII. *John Anderton Smith*, is sufficiently unique for his distinction in a population of a given size, given the probability of existence of another individual with the same name. When the unique attributes apply to many individuals allowing the entire group to be distinguished from the population they are considered Group Identifiable Information (GII). Deoxyribonucleic acid (DNA) profiling techniques successfully determine family relationships such as paternity, maternity and kinships. Grouping this set of identity makers together results in P/GII.

Non-Personal or Group Identifiable Information is a set of PI that excludes identifiable information of an individual or individuals. The set, represented mathematically as $PI - P/GII = NP/GII$, hinders distinct identification of individuals providing only

estimates of their likely identity. Stereotypes are good examples where opinions or beliefs are attached to NP/GII markers such as ethnicity, gender or postcodes.

Sensitive Information are NP/GII that are of intimate or privileged nature which on their own have no impact on the owners, but associated to specific P/GII reveal substantial details about the individual that could be damaging. Health information is amongst the most stringently protected SI and they include individuals' health details such as disabilities, diseases and other health service related information for example organ transplants. Other SI included race, ethnic origins, political opinions, religious affiliations, membership of trade unions and sexual preferences.

Contactable information are PI used for interacting with individuals such as E-mail addresses, residential addresses, phone and fax numbers, IM and Internet Relay Chat (IRC) handles. Contactable information are the preferred PI by marketers as they permit contacting large numbers of users efficiently and may also uniquely identify individuals for follow ups.

However, the most influential PI categories in this study and for personalisation are individuals' S/CI and P/GPref. The pervading environment in which mobile terminal activity occurs, offers enriching PI that characterises its settings as S/CI. S/CI are instrumental in mobile terminals that are often on their owners' possession experiencing similar situational and contextual environment. P/GPref describes PI regarding individuals' decisions and judgements on the valuation of attributes, where the attributes in question may be content, meal or seat types with judgements such as dislike and like. User preferences and their role in personalising services accessed from the mobile terminal are discussed in Section 2.3 along with the wishes of users whose satisfaction should be maximised by providing attributes that match or exceed their expectations.

Catering for users' perspectives on PI implies accounting for subjectivity in PI decisions. Therefore, instances of PI in Table 2.1 divisions are not fixed, but rather flexible and dependent on a specific user. For example, if John composes his E-mail address from concatenations such as *john.smith@email.fi*, he is likely to consider E-mail as P/GII in comparison to Jane's format of *js003@email.fi*. Jane is likely to refer to E-mail as contactable information. Bearing in mind that E-mail addresses are universally unique, but in Jane's case the unlinkability of the E-mail to her person before incorporating additional information from other sources affords her more extra privacy and anonymity than John.

## 2.2 Situation or context information

Mobile terminals, in their owners' possession, often experience precisely the same situations as their hosts. By exploiting this situational and contextual information, mobile terminals gain an important understanding of the user environment resulting in better decisions that are more relevant to their owners. The inclusion of mobile terminal derived S/CI into the decisions of disclosing users' PI to services is an important asset in providing the right PzI to receive the appropriate personalisation and preserve the owners' privacy. Beyond personalisation and privacy preservation, accounting for S/CI minimises embarrassing outbursts by adapting the application's functionality with regards to convenience and cost savings.

The enriching information from mobile terminals PI is similar to how the implicitness of human interactions broadens their communication bandwidth. The increased bandwidth enriches individuals' dialogue on the basis of a shared world view, common understanding, social status, experiences, everyday situations and body language. This enrichment is often referred to as *"speaking the unspoken or reading between the lines"*. Similarly mobile terminals can exploit their host's situational and contextual cues when adapting their functionality. For example, John's mobile assesses his prevailing surrounding, and adapt its functionality to automatically ring when in noisy public places like an airport and silently vibrate when in a work meeting. This situational enriching information of user is termed context by computing and social scientists in numerous formalisations of the concept.

Despite various context formalisms, settling on a concise definition of context is non-trivial. Dourish [37] affirms this by pointing out that *"context is a slippery notion. Perhaps appropriately, it is a concept that keeps to the periphery, and slips away when one attempts to define it."* [37]. No wonder Schilit et al. [136], Wand et al. [148], Adams et al. [135], Pascoe J. [124] and Dey et al. [34] offer various definitions of context. Schilit's definition is among the earliest and relates context to localities and identities of nearby people and objects, and their interchanges [136]. In its incompleteness, Schilit's definition encouraged more scholastic definitions that were either vague generalisations of environments and situations [148, 135], synonyms [124] or too specific for practical use. From the context definitions, Dey et al. stood out.

Dey et al. defined context as *"any information that can be used to characterise the situation of an entity, where an entity can be a person, a place or an object considered relevant in the interaction between a user and an application, including the user and applications themselves"* [34]. This definition has been widely adopted in academic literature. Dey et al. articulates further that *"a system is context-aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user's task."* [34]. Notably, Dey's definition takes a user perspective and therefore, appropriately adopted in this thesis. Two sociological theories that compellingly enlighten the viewing of context from the users' perspective are the positivists and phenomenological theories. These theories explain the need for context in analysing aspects of users' settings. Positivists view context as simple objective and interdependent descriptions explainable *quantitatively and mathematically*. To the phenomenological theorists, context is a property of interactions negotiated, contested and continuously reinterpreted *subjectively and qualitatively* [37].

Positivists and phenomenological views have influenced computing systems developers in their considerations of context as means of engineering users' actions and their relationships with services that will serve them conveniently. The emerging shared perception is that context is an interaction and representation problem based on four assumptions [37]:

1. Context is a form of information encodable and representable like any other information types in computing systems.

2. Within some application frameworks it is possible to define beforehand what the context is and what it is not for activities.

3. Determining context relevant for an activity that an application may support can be done in advance with assurance that it remains the same in the next instances of the activity.

4. Context describes features of the environment within which the activity occurs. Therefore, context and activity are separable. For instance, John might be drinking coffee at Terminal 2. The activity is drinking coffee and the contextual aspect of location is Terminal 2.

Weiser's [150] work is among the earliest to utilise users' context documented in his seminal paper, *"The Computer of the 21st Century"*. This work coined the term Ubiquitous Computing (ubicomp) to imply the calm blending of computing systems in the background of everyday activities exposing intuitive interfaces [150]. Weiser bridged context perceptions by drawing inspiration from Suchman et al. [143] the notion of *"situated actions"*. The focus of situated actions was on improving aspects of human behaviour and discouraging predetermined plans, anticipations and scripts for users to simply execute [150, 2, 143]. This work paved the way for ubicomp and context-awareness research trends.

### 2.2.1 Sources and types of S/CI

To use S/CI from mobile terminals and to implicitly provide personalised and privacy preserving services to users warrants understanding of the S/CI channels. Accounting for all potential sources and types of S/CI improves the quality of decisions on their impact on personal and preference information disclosed from users' terminals.

Ensuing ubicomp literature focused mainly on sensors and users' inputs for S/CI. For example, the 1994 ordk of Schilit and his colleagues [135] focused on the location (*where are you?*), the user (*who are you?*) and the environment (*resources near you*). To Schilit's list, Gross et al. [58] added secondary dimensions of users' S/CI like interests, preferences, knowledge, activity logs, time (for example working hours, on holiday), the environment and current activity in his 2001 study [58]. The most concise listing of S/CI aspects was by Mayrhofer [97] in his Ph.D. thesis in 2004. Mayrhofer's listing specified S/CI [97] to include:

- Geographical (country, street, building, floor, office),
- Physical (ambient light, noise level, temperature, acceleration, orientation),
- Organisational (institution, department, group, project),
- Social (family, friend, work colleagues, marital status),
- Emotional aspects, user (profile, location, capabilities, role, access rights),
- Task (documenting, programming, construction),
- Action (typing, reading, walking, sitting, talking),
- Technological (connectivity, network bandwidth, network latency) and

- Time (time of day, weekday, week, month, season).

Recent trends indicate intensified efforts to solicit users' S/CI from early studies sources, and also to introduce and exploit new sources like on-line communities such as Facebook, MySpace, Linked-In, Friendster and Twitter. The motivation for all this being that on-line communities have become popular and vibrant with users frequently monitoring and using them to interact with others, plan activities, schedule events, post announcements, collaborations, discussions and update their on-line social statuses [13]. This richness of interactivity in S/CI has caught the attention of recent context-aware services.

Situation or Context Information has two distinguishable instances: primary and secondary. Primary S/CI represent lower level details of an activity such as location (*61.067256, 28.090811*) and time (*1400hrs*). However, when these low level instances are interpreted to higher level meanings such as *@work* or *coffee break* they are considered secondary S/CI. In the last decade, context-awareness trends have propagated so as to enable mobile terminals to more accurately sense their owners' S/CI and disclose them to services [27, 125]. Mobile terminals are now capable of precisely determining their hosts' primary and secondary S/CI. Instances of primary S/CI mobile terminals can be determined from their hosts' include locations, identities, plans and activities, while those of secondary S/CI derived from the primary instances include, *@home* or *@work* [1]. On-line communities have also emerged as significant source of secondary S/CI under titles such as "status, activity, what's on your mind? Or what's happening?" Overall S/CI channels have broadened to include other terminals (desktop computers, laptops and mobile terminals), sensor (in-built, environmental) and on-line communities as illustrated in Figure 2.1.

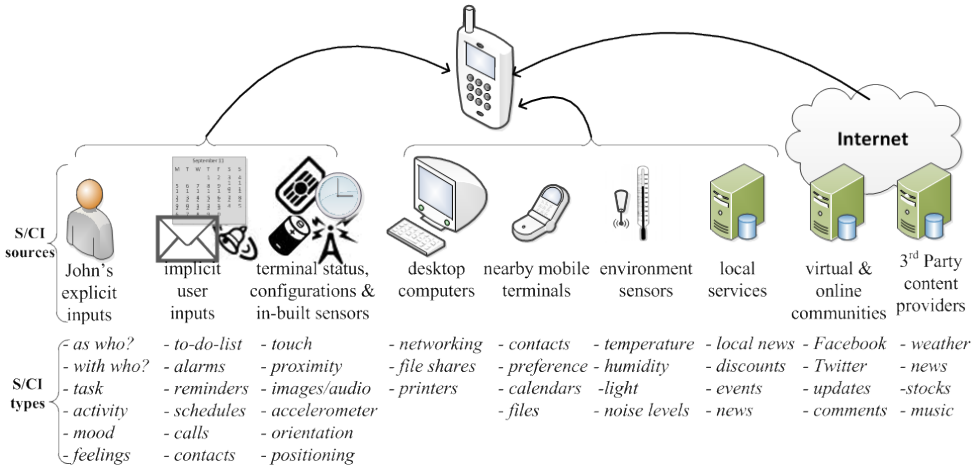



**Figure 2.1:** Sources and types of S/CI available to mobile terminals.

The sources in question include audio, image, touch, proximity, biological sensors and GPS receivers. Mayrhofer's listing includes S/CI types such as ambient light, vision, acceleration, location, orientation, proximity, environmental, gravitational force, identities and state changes [97]. Figure 2.1 depicts some sources and types S/CI related to current

mobile terminals. These sources are increasingly becoming more intimate and personal to the user from right to left.

In this study, the subset of S/CI accessible from users' mobile terminals includes what the user provides directly and indirectly to mobile applications. Other sources of S/CI may be the user's desktop computers, terminals belonging to others the user comes in contact with such as friends, spouse or work colleagues. Directly entered S/CI might include statements such as *shopping, gift, anniversary, at work, vacation, business-trip* or *bored*, while implicitly inferred S/CI statements include mobile terminal reminders, to-do-lists, alarms and calendaring.

### 2.2.2 Modelling S/CI of users

Once the S/CI of the user has been determined in the mobile terminal, they have to be incorporated into the terminal's applications that can actually utilise them to affect the users' PzI. The incorporating of PzI into applications enables their adaptability to the individual situation and eases the application's evolution as it caters for different user situations. Incorporation of S/CI is a complex task. This is why formal modelling S/CI in a logical manner that facilitates consistency and reasoning checks is required. Modelling also aids in translating real world concepts into languages understood by users and developers and allows computational reasoning on S/CI for performance and scale considerations. Various S/CI models and proposals exist that are suited for different application domains (Figure 2.2).

Bettini et al. [18] and Emiliano et al. [126] emphasise the importance of selecting an appropriate S/CI model for a user accessible service that depends on its domain needs and fulfilment of the following requirements:

1. **Heterogeneity and mobility** - Various S/CI are sensed, provided by user implicitly and/or explicitly. Portions of this information are in heterogeneous raw formats (22° Celsius, 77° Fahrenheit, *warm*) and others are updated more frequently. These inconsistencies should be addressed before using S/CI in applications [126].
2. **Relationships and dependencies** - S/CI often has relationships with other S/CI that should be captured. For example, outdoor activities like jogging or swimming might be related to warm weather, daytime or summer activity while, indoor activities like table tennis and board games might be related to night time, winter season or cold weather. Applications changing one aspect of a users' S/CI are likely to affect other aspects of S/CI as well.
3. **Time-lines** - Situations change often in mobile environments, hence, they must be promptly captured and stored for historical purposes like predicting and anticipating future situations. Frequently updated S/CI should also be aggregated and summarised [126].
4. **Quality and accuracy** - Sensors are often accurate within some margins of error. For example, GPS receivers are accurate within 10 - 20 meters depending on satellites constellation and if the receiver is in an urban or open landscape. The reliability of these sensors might also vary, resulting in incomplete or conflicting data that have bearing on their quality and accuracy [18].

5. **Reasoning** - Applications reason on S/CI to determine if there is a change in the situation and make an appropriate decision. This determination should be consistent and verifiable.

6. **Usability** - It should easy for service developers to translate real world concepts into modelling constructs. This ease should also apply to applications using and manipulating the users S/CI at runtime.

7. **Efficiency** - Applications should have reasonable access time to relevant primary S/CI [18]. It is pointless to recommend a suitable restaurant serving John's preferred meal long after he is seated and placed at a less suitable restaurant.

Motives for proposing S/CI models vary from simplicity, expressiveness and support for reasoning on a single aspect such as time or space. Combing these reasons and their emphasis on different modelling aspects results in the six dominant S/CI models depicted in Figure 2.2.

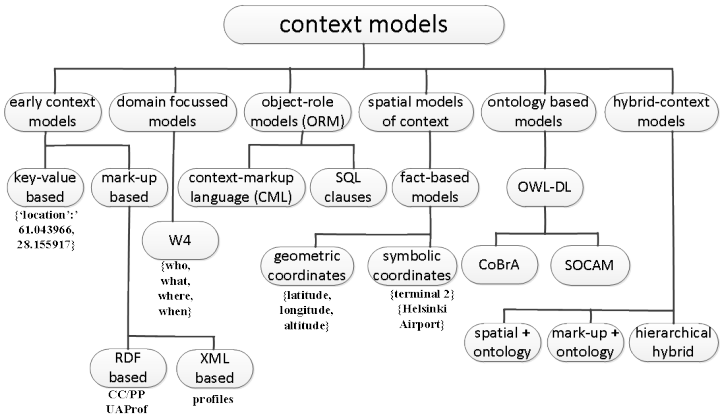



**Figure 2.2:** Classification of approaches to S/CI modelling

Early S/CI models were either key-value or mark-up based. Key-value models encode contexts into tuples of data with unique identifiers, while mark-up use an Extensible Mark-up Language (XML) basis to depict constraints and relationships between elements. The key-value models are incapable of capturing S/CI varieties, relationships, dependencies, timeliness, quality, consistency checks, reasoning on context and higher abstractions. This incapability renders key-value based models infeasible to address domains relationships between user situations, PI and preferences and PI. S/CI models may also be specific to domains, for instance, W4 supports representing query tuple *{who, what, where, when}* but fails on *how* and *which* [18].

Efforts to maintain backward compatiblity with legacy data led to relational database inspired models. Relational database inspired models [126] or Object-Role Model (ORM) [65] store preconfigured preferences that can be queried using Structured Query Language (SQL) clauses [126]. Hendricksen's [65] Context Modelling Language (CML) is one realisation of ORM that enables the conceptual modelling of databases with graphical notions

[65]. ORMs are suitable where S/CI relevancy is predefined or the applications functionalities are limited to S/CI dependent on data retrieved [126]. ORM has some benefits in modelling S/CI in mobile terminals, however careful considerations have to be taken into account given that some terminals lack relational databases based on SQL.

Spatial context models emphasise space in context-aware applications on a fact basis to organise information by their physical locations. The location is predefined with static entities and obtained at runtime via positioning systems in mobile terminals. Geometric coordinates (*latitudes, longitude, and altitude*) and symbolic coordinates (*T2 at Helsinki Airport*) are the supported locations. Spatial models allow reasoning in terms of distinct area, range and distance to entities [126]. Spatial S/CI models have bearing on mobile terminal domains with minor improvements that would allow them to cater for other types of S/CI.

Ontology Based Model (OBM) defines relationships between concepts that can later be used for reasoning by exploiting the expressive power of description logic to [126]:

- Describe complex S/CI not representable in other models.
- Formalise S/CI semantics in a manner that facilitates their sharing or integration.
- Provide tools for verifying the consistency of a context scenario.
- Recognise the activity in which the S/CI is related.

OWL-DL [67] is a formalism of OBM standardisation supported in many application domains. By using OWL-DL a specific domain is modelled by defining classes, individuals, individuals' characteristics and relationships between individuals, thereby, allowing the composition of new elements from the existing one [67]. OWL-DL models have been adopted by a number of other context-awareness models like, Context Broker Architecture (CoBra) [77] and SOCAM [15] middle-ware. Unfortunately, OWL-DL suffers from three limitations. First, it is limited in expressing constructs that model complex domains like user activities. Second, some of OWL-DL's context domains are problematically prone to conflicts as the concepts and relationships must be built and agreed upon by a set of users. The problem arises from the difficulty of providing a general enough ontology to model any context effectively. Third, OWL-DL is computationally expensive [18]. These limitations of OBM amplify mobile terminals constraints when processing, memory and power directly and therefore require serious consideration before adoption.

To mitigate the limitations of specific models, scholars have combined different S/CI models to maximise the benefits and/or strengths of one model while minimising the limitations of the other. These integrated models are termed Hybrid Context Model (HCM). Some benefits of S/CI models to be maximised include interoperability, good support for software engineering and heterogeneous support of other models. For example, spatial models are known to be highly interoperable with other spatial models, while ORM are said to have good support for software engineering processes. In addition, OBM can be useful in improving the interoperability and heterogeneity of other models. Some examples of HCM have resulted from combining spatial and ontology models, as well as mark-up and ontology models. In this study, a mark-up and ontology hybrid model is adopted for its suitability in modelling S/CI from user's mobile terminals and their P/GPrefs.

### 2.2.3 Life-cycle of S/CI

Irrespective of the S/CI type, source, modelling strategy or usage scenario, a user's S/CI has a distinct life-cycle. At the time of sourcing the S/CI it more significant in decision making and later in its life-cycle S/CI is less significant if not irrelevant in any decision activity. The life-cycle is divided into the phases of acquisition, reasoning and decision actuation as Figure 2.3 depicts. At the acquisition phase, raw measurements from various S/CI sources are stored in heterogeneous formats. The heterogeneities of the raw inputs such as temperature (°C or °F) mandates their representation into standardised formats then to higher abstracted formats like *warm* or *cold* to enable their fusion, summarising or reasoning by upper layers.

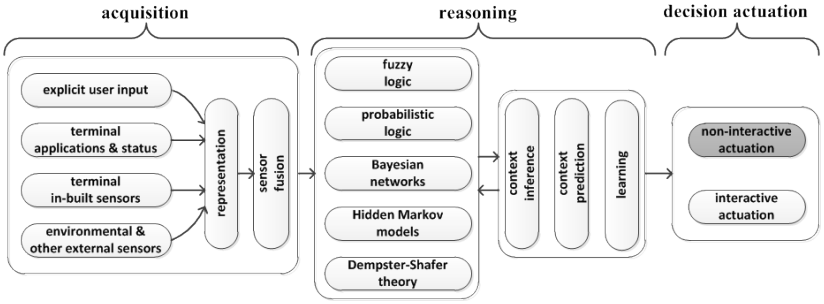



**Figure 2.3:** The life-cycle phases of users' S/CI.

In the reasoning phase, conclusions are deduced from rules and preconditions of lower level facts. For example, *when it is cold weather, drink warm beverage or when it is warm weather, drink a cool beverage*. Inferences are conducted on uncertain, incomplete and often inaccurate information using a variety of algorithms. Compromises in computational complexity, accuracy and users experiences are made in this reasoning phase. The third phase of S/CI life-cycle is the actuation phase. Actuation types distinguished as *non-interactive* and *interactive* actuations. While non-interactive actuations automatically adapt the applications behaviour to the detected S/CI, interactive actuations present the user with the detected S/CI demanding their explicit permission for their final decision. To facilitate transparent service provision, non-interactive approach is adopted in this thesis.

### 2.2.4 Using S/CI of individuals

When individuals disclose their S/CI to ubiquitous services, it gives the services four dominant utilisation scenarios. In the first scenario, the services may incorporate individuals' S/CI with other relevant information to aid in **searches and retrievals** of other information items as clues or hints. Figure 2.4*(a)* depicts the first scenario as the meal locator takes into consideration John's S/CI pieces (*@airport, cold weather, Tuesday morning, departure time, supervisor role*) to search and return an appropriate meal or beverage for the given situation. Some implementations adopting this scenario include Lifestreams [47] and Forget-me-not [84].

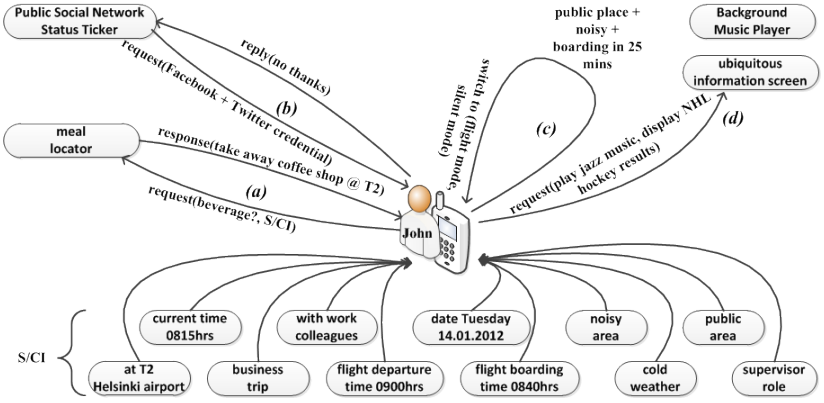



**Figure 2.4:** Dominant utilisation scenarios of S/CI from mobile terminal.

In the second utilisation scenario (Figure 2.4*(b)*) John's S/CI are used to dynamically determine the mobile terminals *interaction behaviour with services* at service access time. In Figure 2.4*(b)* John's mobile terminal receives request from a public ubiquitous screen for his SN credentials (Facebook and Twitter) to update his status automatically. After considering John's current S/CI (*business trip, supervisor role, with work colleagues*), his mobile terminals declines the request as inappropriate. Implementations adopting this usage scenario include Easy Living [22] and Electronic Tourist Guide [28].

The utilisation of an individual's S/CI by the mobile terminal in determining its **functionality** formulates the third scenario depicted in Figure 2.4*(c)*. John's mobile terminal bases its decision to switch to silent and flight mode from ringing mode on, S/CI of *public places, noisy, current time* and *boarding time*. In the fourth utilisation scenario, the mobile terminal takes into account an individual's current S/CI to **determine or limit** additional PI that may be disclosed. In Figure 2.4*(d)*, John's mobile terminal considers his personal preferences and accompaniment to disclose his likes for jazz and ice-hockey to the information screen.

In combining these four utilisation scenarios, individuals' S/CI may be used in a hybrid manner where their S/CI are used to aid in information searches and retrievals. Additionally, their S/CI might be used to limit what PI items are disclosed as well as adapting a certain terminal and the service functionalities. This hybrid utilisation scenario is adopted in the Conference Assistant [34] and is the strategy followed by ME2.0 to the extent of limiting PI disclosures.

## 2.3 User preferences and personalisation

The PI in mobile terminals today contributes in overwhelming users such that they may struggle to make appropriate decisions. Nonetheless, these decisions are subjective matters that possibly vary across individuals and situations. Assuming, there is a known appropriate decision, an aggravating factor that is likely to limit users arriving at that decision is their limited ability to process all the information in the short amount of time they divert to focusing on their mobile terminals. Taken together, these factors are

likely to hinder consistent appropriate decision making. Simply put, limitations in the cognitive capacity of individuals constrain their ability to make appropriate decisions always. Otherwise, privacy discussions would not be necessary. The results of sub-optimal decisions often include overestimates or underestimates of risks and privacy implications associated to the particular PI item or their disclosure.

By filtering the PI in a mobile terminal as well as what is presented to the user, this study reduces the amount of processing and attention demanded from the user, thus increasing the probability of arriving at the right decision. Additionally, filtering reduces the effort users need while easing and ensuring convenient interaction with their mobile terminals that are aligned with user orientation perspective which is one of the main gaols of this study. Fundamentally, the role of preferences in this study are to reduce the information overload on the user, while providing him with relevant information that requires minimum processing and attention so as to remain relevant and limit avoidable privacy invasive disclosures to services.

User preferences are the wishes of a user. While it is possible to maximise user satisfaction with user preferences, complete fulfilment cannot be guaranteed [6]. These user wishes are not readily available, despite being essential components of successful provision of personalised services. The positive correlation between user preference and personalisation is the motive for considering them alongside each other. High quality user preferences enable a mobile terminal to disclose better positioned PzI to services and thereby obtaining higher quality service personalisation. The significance of user preference in personalisation is seen in personalised entertainment [93], query enhancements [80], Digital Libraries (DL) [48, 8], personalised websites [54], delivering personalised service in smart environments [81, 44] and in the building optimal sets of team in gaming domains [33].

In composing a music play-list in a mobile terminal, the most obvious solution is to rank all music tracks then select the top $k$ items. This preference determination approach yields sub-optimal subsets, a phenomena termed the *"portfolio effect"* [24] or *"dependent relevance"* [155]. John's favourite music artist, *Miles Davis* might rank first in the list, but he might not want to compose and listen to an entire play-list consisting of only this artist's music all the time. John is likely, to appreciate more a play-list comprising other jazz artists or music genres. Such inadequacies of structuring user preferences for suitability in different domains or to ensure that they yield optimal solutions all the time have been addressed by various scholars, for example DesJardins et al. [32] and Mukhtar et al. [105]. DesJardins et al. tackle the challenge by proposing "DD-PREF" a language for expressing user preferences over sets before proceeding to extend DD-PREF in [33] using a greedy algorithm to account for the portfolio effect while returning the most satisfying sets.

Mukhtar et al. focus on users' preferences in accessing services using different mobile terminals. In [105], the starting point is users specifying their preferences qualitatively with positive notions of *likings* or negative notions of *dislikes* specifiable at different levels of relative importance (Figure 2.5*(a)*). For example, *John likes hot tea* or *John likes hot coffee more than cold tea.*

To capture the notion of *more important* and the notion of *less important*, a mapping of *preference* $\mapsto$ *importance level* is introduced. The mapping allows the quantitative

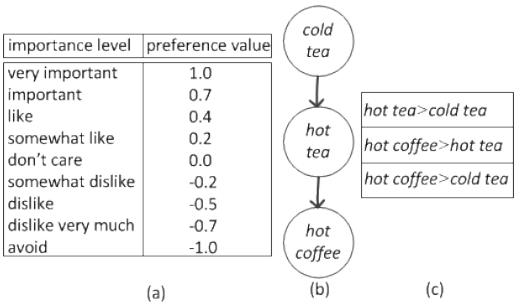



**Figure 2.5:** Values for preferences and CP-net example.

specification of users' preferences, maximum, minimum and closest match [105]. Conditional Preference network (CP-net) [21] model is employed to compact the representation of conditional and qualitative preference relations (Figure 2.5*(b)*). Each CP-net has an associated Conditional Preference Table (CPT) which expresses the preference it takes over values. Preference between two outcomes, *hot coffee* and *cold tea*, can be specified by the $\succ$ relation (Figure 2.5*(c)*). Such that, *hot coffee*$\succ$*cold tea* specifies that *hot coffee* is preferred to *cold tea* [106, 104].

The user preference approach in [105] has bearing on mobile terminals with respect to the users qualitatively specifying their positive and negative notions of personalisation content. The qualitative specification and the capturing of more important or less important notions are adopted in this study to rank users preferences in composing their PzI that are disclosed to services. The implications of this approach result in means of mapping users' privacy expectations on PI items and in determining the disclosure decisions.

Hierarchical preference trees [93] and rule-based languages approaches [44] are other approaches to model user preferences. In hierarchical preference trees, the focus is on the user's long term static service preferences without consideration for spontaneous preferences that depend on the context of use. Contrastingly, rule-based approaches account for the context of use in users preferences of desired personalisation. Liu et al. [93] modelled user preference on a two-layer tree combining the hierarchical and rule-based approaches. In [93], user preferences for personalising services are composed of the users' long term static commitment to certain kinds of services and, spontaneous service requirements that depend on the context of use. Users static preference are composed by a set of preference items represented as an attribute/value pair (*entertainmentType, music*) that could be further refined to (*genre,jazz*) sub preferences as Figure 2.6 depicts [93].

Kodoma et al. [78] also proposes a restaurant recommending application for mobile terminals that takes into account the host's current location and preferences. In this proposal, a user's profile records preferences in relative order within predefined categories such food types, location and prices [78]. The authors advance the approach adopted by many recommendation systems that use the user's location and distance to the nearest service to make the decision.

Liu et al. study [93] has relevance in organising the User Interface (UI), in this study to

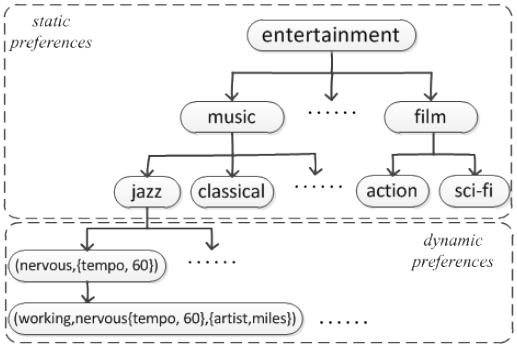



**Figure 2.6:** A model of user preference instances [93].

capture preferences within a contextual bearing. The approach presented in [93] shares more in common with the mobile terminal domain presented in this study, in comparison to the proposal in [78]. The deciding factor is the consideration of static commitments to select services while accounting for spontaneous personalisation based on S/CI.

### 2.3.1 Service personalisation

By focusing on the user, the goal of the study is to make it conveniently easy to for users to obtain personalised services. Given this, the techniques that services adopt to personalise their offerings to users are out of the scope of this thesis. However, these are briefly discussed here in order to put into perspective what PI items are utilised and how the PI are handled, thereby providing some reflections on privacy preservation.

The term 'personalisation' is often used interchangeably with *adapting, tailoring* and *customising*. However, the difference between these terms need clarification. The Oxford Advanced Learner's Dictionary [66] defines these terms as given below:

- **Adapt** - Make something suitable for new use or situation. *This machine has been specially adapted for use underwater.*
- **Tailoring** - Making something for a particular purpose, person or type of person. *Homes tailored for the needs of the elderly.*
- **Customising** - Altering something to the buyer's or owner's wish.
- **Personalise** - Mark something to show that it belongs to a particular person. *Handkerchiefs personalised with her initials.* Or cause something to be concerned with personal matters or feeling rather than with general issues [66].

From these definitions, *personalise* and *customise* are most appropriate in this thesis considering the use of PzI and the role of user preferences. However, consistency dictates the discussions in this thesis are restricted to *personalised* terminology.

According to Perugini et al. [127] personalisation is the *"automatic adjustments, re-structuring and presentation of tailored content to individuals"*. Kuo et al. [83] and Liang

et al. [90] emphasise the presentation of appropriate content and services, based on the knowledge of user's preferences and behaviours. The significance of *correct information*, *the right time* and *the right manner* are also emphasised in [88]. Deductively, these works arrive at the same motivation for user preferences in mobile terminals, i.e. that the main purpose for personalisation is to limit exposing users to overwhelmingly large numbers of options by filtering out the irrelevant, based on their interests. Liang et al. [90] consider a personalised system, as one building on user profiles from past usage behaviour to provide relevant services retrieved from large repositories to users. This consideration raises the need to create user profiles, model the service, and filter the data.

Personalisation techniques adopted by systems have evolved from obtrusive systems that greeted users by their names to current unobtrusive systems. The evolution has accompanied adoption of personalisation in DL [48, 8], E-learning [151], E-commerce [83], news or information recommendations, search engines and applications [50], many of which can be accessed from mobile terminals. In the adoption domains, unobtrusively personalised services are seen as solutions to rising demands for customer-centric services and the declining number of loyal customers. Loyalty among customers is likely to increase as services recognise, understand and attend to their customers' unique needs. Thus, service providers employ various collection channels such as E-mail, websites, call centres and physical stores, to collect heterogeneously formatted PI from users. There is an inherent challenge in integrating, synchronising, verifying, correcting and frequently updating users' information.

The situation is different in ubiquitous services that personalise their offering to their users. Disclosure of PzI by users is highlighted from the perspective of the mobile terminal and the four personalisation phases depicted in Figure 2.7.

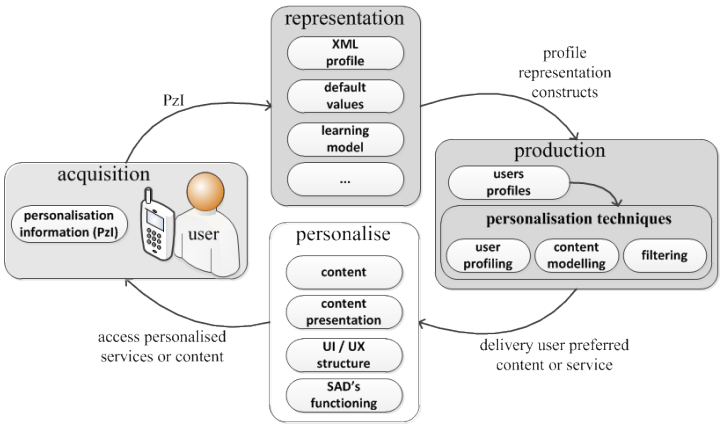



**Figure 2.7:** Phases of personalisation in ubiquitous services

Figure 2.7 acquisition phase, results in PzI that are solicited from the user explicitly or implicitly. The PzI are then represented using models to support interoperability in the representation phase. Based on the representation, user profiles are then constructed and used in the production phase with machine learning techniques to personalise service. The 'personalise' phase, raises questions of *what aspects should be personalised* and *how*

*this should be achieved.* Candidate areas for personalisation in the mobile terminal are:

- **The content** - Recommend *Moe's Take-away coffee shop at Helsinki Airport T2 to John.*
- **The content presentation** - Display a text list of Moe's coffee shops prices, graphics with links to the web pages or speech output for visually impaired persons.
- **The UI/UX** - Change John's terminal's layout and navigation to cater for his current preference, the terminal's limitations and the environment. The importance of usability cannot be over emphasised, it must always be about the user [16, 53].
- **The mobile terminal's functioning** - For example, based on John's price preferences, the use Bluetooth or WLAN rather than 3G, or while abroad data connections could be severed as they are expensive.

In this study, the main personalisation candidate is the content which might be delivered to the user's mobile terminals or displayed on a public space such as the information screen. Critical to personalised ubiquitous services is the mapping of user's preferences and the ubiquitous services that serve them. Personalisation techniques mainly realise this mapping based on the user's profiles.

### 2.3.2 Personalisation techniques

The main personalisation techniques are based on user profiling, content modelling, and filters as Figure 2.8 presents [50]. Often users select services *interactively*, from *recommendations* or *inferences*. The selection criteria are useful in determining the appropriate personalisation techniques to be implemented [56]. However, the most often employed technique is filtering, or more specifically, Content Based Filtering (CBF) and Collaborative Filtering (CF).

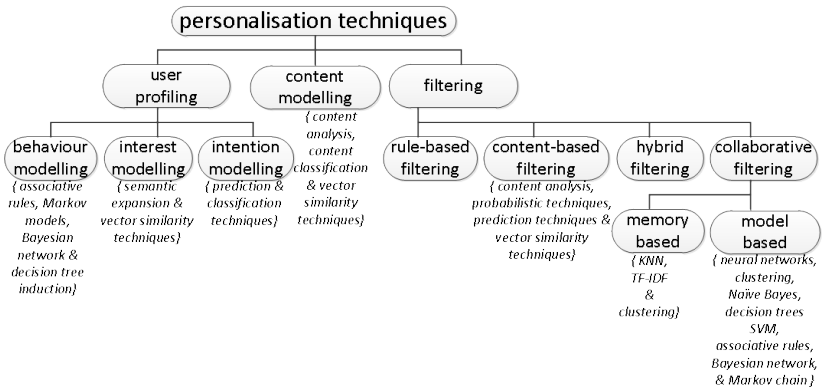



**Figure 2.8:** Personalisation techniques [50]

CBF is based on a user's previous preferences, while CF exploits preferences from similar users or groups on which to base their personalisation [56]. Both techniques have

limitations leading to their integration to formulate hybrid techniques such as mitigation strategies.

Rule-Based Filtering (RBF), the simplest filtering technique uses user static profiles to specify *f(user, service)* rules. Pre-defined *IF/ELSE, AND/OR* rules are then applied to determine the appropriate decision [50]. Behaviour modelling attempts to discover patterns from services usage by users to determine an effective strategy. Interest models build users' preference functions *(pref(tea))* of how much a user likes or dislikes the item *tea* by analysing their historical behaviours. Intention models attempt to determine the user's *purpose, goal* or *aim* [48, 50]. Content modelling techniques use key indicators on services or content expressed as meta-data that is used to select relevant instances. These instances are often documents or service contents and are classified using vector representation algorithms [50].

Regardless of the personalisation technique adopted and used by a service, the amount of precise PI from users and their privacy implications are only determined after the services have collected and analysed their PzI for some time. Therefore, by focussing on the selection of PzI prior to disclosure, the amount of PI leaked can be regulated thereby, limiting their link-ability to specific users. The manner in which services handle PzI is important in order to understand how PI leakages could occur.

### 2.3.3 Handling PzI

The storage of consumers' S/CI and their preferences in their mobile terminals, and their subsequent disclosure to services implies that the consumers would be able to access personalised services any-time, anywhere using various heterogeneous mobile terminals and still retain the service relevance. Along with this, would be the increased potential for consumers to disclose PzI with implications on their privacy. To minimise disclosures with privacy implications, considerations to the handling of PzI by mobile terminals are required to retain their relevance, trigger personalised services and minimise PI leakages.

What consumers and services consider PzI in the mobile terminals are also bound to evolve by incorporating newer or additional S/CI with user preferences. For example, consumers' preferences are bound to account for aspects such as their location, speed, direction and environment. Terminals used to disclosing PzI are becoming more heterogeneous in terms of capabilities, networking and functionalities.

The manner in which consumers will interact with services from these heterogeneous terminals will become increasingly goal oriented as opposed to exploratory as with World Wide Web (WWW). This is due to the fact that consumers accessing these personalised services will mostly likely be engaged in other tasks at the same time such as driving or eating.

In handling the PzI related to disclosure to services, the role of S/CI in the mobile terminal and in this study are pivotal. In this study S/CI is used to select the appropriate user preference to disclose in a given consumer-service interaction. The appropriateness is evaluated in terms of received personalised services and the perceived preservation of the individual's privacy. Therefore, the solution in this study uses S/CI to notate PzI from users in a specific situation. This reveals possibilities of isolating PzI and S/CI in a manner indicating that consumers should only disclose Context-Notated Preferences (CnP)

to services and still access similar personalisation as previously. Figure 2.9 illustrates the isolation of P/GII, P/GPref and S/CI in the context-notation concept.

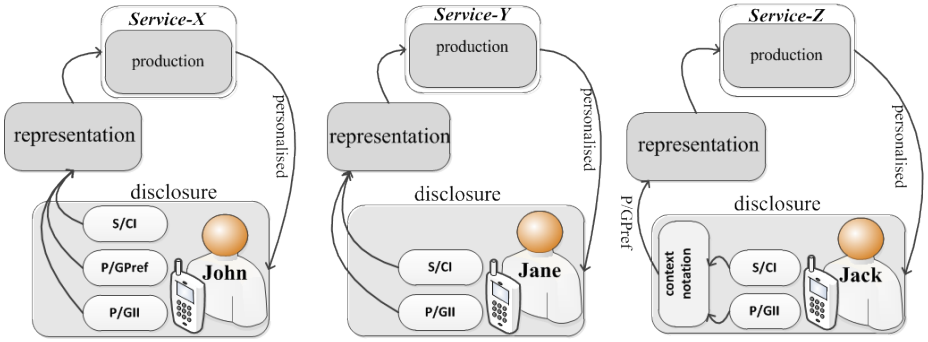



**Figure 2.9:** Context-notation

In Figure 2.9, John discloses to *Service-X* some of his PzI of the types P/GII, S/CI and P/GPref, in order to obtain personalised services. The situation with Jane differs slightly in her disclosure of P/GPref and S/CI, opting not to disclose her P/GII. In Jane's case $Service - Y$ has to infer her preferences using profiling techniques. Jack notates his PzI with his S/CI to determine the P/GPref, disclosing only his P/GPref in the prevailing situation to services. In this sense, $service - Z$ is incapable of fully identifying Jack directly as it lacks a sufficiently unique identity to associate P/GPref to a specific user's identity, $service - Z$ can only speculate on the S/CI upon which the disclosed P/GPref was determined. Based on the user's disclosures, Table 2.2 distinguished services on their handling of PzI.

**Table 2.2:** Services distinguished by their handling of PzI

| service types | PzI handled | | |
|---|---|---|---|
| | S/CI | P/GPref | P/GII |
| A(like *Service-X*) | | | |
| B | | | |
| C(like *Service-Z*) | | | |
| D | | | |
| E | | | |
| F(like *Service-Y*) | | | |

Services A - F are suited to different user scenarios and service architectures. Reflecting on our running example of John at Helsinki airport with S/CI (*@T2, @0815hrs, business trip, boarding at 0840hrs, cold weather, with work colleagues*), P/GPref (*beer, sports cars, wine, jazz, hot coffee*) and P/GII (*phone number, E-mail address, names, SN and payment credentials*). The fact that this study is grounded on personalised service provision mandates the provision of at least P/GPref. Therefore, non-disclosure and disclosing only P/GII contradicts the concept and are therefore omitted from Table 2.2. In service

A, John would disclose their entire S/CI, P/GPref and P/GII delegating the notation to the service to determine the appropriate meal and location in his current situation. The presence of P/GII in service A raises privacy concerns. Therefore, omitting them would result in providing the service with John's current situation and preferences to determine the appropriate meal as with Service B. The resultant personalisation with Service D and F are almost identical as they lack John's P/GPref basing their personalisation primarily on John's S/CI. Services C and E provide desirable personalisation with the former preserving John's privacy more. This thesis aims to position its mobile terminal solution to accessing personalised services of type C.

Personalised ubiquitous services are a challenge to design, develop and deploy. Paradigms used in developing desktop application are insufficient to satisfy mobile terminals' UI considerations, due to the terminal's inherent characteristics, the services they access, and their personalisation. A common means of limiting the complexity of development is to use compact web pages restricted to mobile browsers and using a device independent auto-generated UI from XML constructs. Even so, selecting the most appropriate service matching the users' functionality, Quality of Service (QoS) and privacy requirements remains a deployment challenge. These challenges raise complexities in discovering services, logical interoperability between services and the execution of selected services.

## 2.4 Privacy implications

An increasing number of users are becoming progressively more conscious of the need for personalisation to collect amounts of PI about them. Surveys by ChoiceStream on consumer trends and perceptions towards personalisation reveals that 79 percent of users are keen on personalisation, 57 percent are willing to trade-off some of their PI like demographic, preference and transactional information for more personalised content [76]. In addition, personalisation is considered vital to SN experience by 75 percent of respondents, and 33 percent of users are willing to received personalised advertisements. The top five sought after personalised services involve books, music, films, television, web search, and news or events [29]. Despite the surveys suggesting that personalisation is on the rise, privacy remains a major concern [29].

Nonetheless, privacy remains an ill-defined but well understood concept. Ill-defined because the term privacy is often used to mean and imply different things. The concept of privacy is viewed as well understood by those using the term often belief that others share their view. For instance, privacy and anonymity may be considered synonyms. However, distinction between the two clearly emerges in Information Technology (IT). Privacy corresponds to John sending an encrypted E-mail to Jane. But anonymity corresponds to John sending the same E-mail to Jane in plain text but without any information that could enable Jane or anyone else to identify the sender. The focus of privacy in this study is aligned to information flow rather than physical privacy. In this regard, Westin's [5] consideration of privacy as *"the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"* becomes relevant. In particular solitude (freedom from observation or surveillance), intimacy (closeness among small groups), anonymity (freedom from public identification) and reservation (freedom to withdraw from communication) are emphasised. [147, 5]

### 2.4.1 Privacy concerns

In contemporary societies, user privacy is perceived in relation to the community, corporates doing business in the community, and agencies governing the communities and corporates. Society is increasingly demanding more PI of their citizens in order to participate in societal activities and access personalised services. To be insured or receive healthcare, citizens must disclose proportions of their PI. Financial institutions packages are also personalised to consumers' investment profiles composed from data mining users' PI. This trend of increasingly demanding more PI from users is compounded as society domains players that were previously isolated such as healthcare, insurance, banking, law-enforcement and education "co-operate" in sharing PI to provide seamless and efficiently personalised services to users [147]. For instance, to qualify for life insurance, one might be required to take a medical examination with the insurance firm's prescribed doctor. Similarly, banking and educations institutions may cooperate with law-enforcers to curb fraud or detain rowdy students.

The privacy concerns involving mobile terminals can now reach further into private life as they are based on users' profiles, usage patterns and user situations. Users can now be continuously tracked, observed and contacted by their pervasive environments and services. Personalised services from the mobile terminals perspective implies that service-user relationships are stripped down to a one-on-one basis. This stripped down relationship has needs for unique user identifiers. Such identifiers enable the behaviours of groups of users to be automatically collected, stored, warehoused and intensively analysed. In ubiquitous services, and long-term identifiers enable services to distinguish, track, log and profile individuals and groups, building accurate behavioural patterns. The emerging rule of thumb is, the longer a user accesses a service the higher the precision of their user profile and personalisation.

Initiatives for Single Sign-On (SSO) identifiers that can be used to verify one's credentials across Internet services have matured, for example, the Liberty Alliance Project [91], Kantara initiative [75] Windows Live ID [101], Windows CardSpace [100] and OpenID [114]. Some SSO solutions such as Live ID, have been integrated with mobile terminals. These initiatives are enabling mechanism towards users PI sharing across services that raise two worrying questions. Firstly, where do users privacy preferences fit in? Secondly, how is mutual trust evaluated between services in controlling the propagation of users' PI?

On the problems of personalised services, Ashman et al. [10] details five faults. First, the reliability of personalisation hinges on constructing user models for complex human behaviours. At best, these models are approximations limited by the accuracy of the algorithms on which they are based, especially when faced with incomplete, inaccurate, and inappropriate user information. Second, personalisation robs users of the feeling of being in control of their own experiences. It thus undermines the learning process by limiting the user's own information filtering process and choices by providing or making the information readily available. Third, personalisation is bound to have inconsistent presentation and outputs of services, considering the dynamic nature of user behaviours and attitudes. Fourth, personalisation is not needed to build effective educational systems, a domain where it is most widely used. Fifth and final is the question of privacy and security, which Ashman et al. have raised and is of importance to this study [10].

The concern that Ashman et al. have raised are genuine and relevant to this study in numerous ways. This study has taken a user perspective orientation to explore how personalised services can be provided to users without compromising their privacy. This research goal contradicts the second and the fifth concerns raised by Ashman et al. The goal of giving users mechanisms to rationally make sound decision on their disclosure by filtering out irrelevant information based on their preferences and situations imply that steps are taken to minimise the inconsistencies and improve reliability. Unlike Ashman et al.'s justification on the irrelevance of personalisation in educational domains, in the mobile terminal's it is an important asset in easing users' lives. By implementing the solution from the user perspective, steps are taken to provide opt-outs that include switching off the personalisation engine, hence bringing down the informational filters.

Privacy concerns involving personalised ubiquitous services revolve around what happens to the amounts of PI solicited by service and used to compose user models that facilitate personalisation. The concerns raise the following questions:

1. Who keeps and owns the records of consumers' PzI?
2. Can consumers view and correct their solicited PzI?
3. What happens if the PzI is released deliberately or acquired through malicious means?
4. What inferences or user models are created regarding users while accessing a service, especially if this is done without their knowledge? Such inferences are bound to have grave privacy consequences when considered from political and social perspectives.
5. What associations are created? A side effect of personalisation is that it creates associations even where non-explicitly existed. For instance, recommending jewellery or romantic holiday to John and Jane might be misplaced especially if they are only work colleagues with no romantic involvements.

### 2.4.2 Threat scenarios

In the various stages of composing and disclosing their PzI to services, a user's PI might be compromised. Threat scenarios are useful in depicting assumptions of privacy compromises by irresponsible and malicious entities. This study focusses on threat scenarios exposed when individuals access services non-interactively or transparently receive personalised offering. Such privacy threats may result from the leakage of users' PI directly or indirectly while accessing the personalised services.

Direct leakages occur when an individual discloses their PI that can be used to compromise their privacy. For instance, providing ones E-mail address to service and then later receiving spam messages to that address can be one form of direct leakage. Indirect leakages are associated with legitimate services inferring other privacy invasive PI from legitimately disclosed PzI or data from other sources. For example, by analysing users' service access locations a service might be able to determine a user's home or work postal codes. Direct leakage of users' PI can be attributed to limitations in the usability of the mobile terminal application in providing users not only with access authentic services,

but also with the capacity to manage the disclosure of their PzI to limit privacy compromises. The importance of transparency and explanation of personalisation features along with their privacy components to users are likely to restore trust when presented with evidence from reputable sources and prevents giving users a false sense of security.

Indirect PI leakages can be categorised into acquisition, representation, interpretation, interaction, and usage. Acquisition leaks are relevant where user credentials are required to access S/CI from environmental sensors or to respond differently to certain situations. Auditing sensors logs can reveal usage patterns that expose the user to surveillance and profiling. Similarly, falsifying S/CI could lead to the user mobile terminal into disclosing their PI to malicious entities. For instance, if Jane's mobile terminal detects her involvement in an accident (from accelerometer and GPS readings) it discloses her PI such as name, age, blood group, medical insurance details, allergies and so on to any device identifying itself as paramedic. If Mallory can mimic an accident scenario (by knocking Jane's mobile terminal down) and then configure his mobile terminal to claim to be a paramedic, then he could obtain sensitive PI from Jane's terminal. If a service interprets users S/CI into easily accessible and comprehensible (*@home, John+Jane*) formats and does not sufficiently conceal them, they could reveal details a user would prefer kept private such as anonymous encounters and discrete association.

Interaction leaks relate to wireless medium threats and their exposure to malicious attack on the medium without attacking the mobile terminal or the services. Medium threats included eavesdropping, message interjection, message modifications and Man-in-the-Middle (MITM). Users are exposed to usage leakages when services excessively solicit PI from users, permitting them to infer more private information.

It is also possible for service providers to process, disclose, sell, indefinitely store, or repurpose users' PzI in manners that contravene their owners' privacy expectations and the services initial reason for collection. Therefore, from the users' perspective key privacy questions that need to be raised and addressed include:

- How much PzI do services really need? Can this be determined in advance or hindsight and disclosures restricted accordingly?
- Of the disclosed PzI items which are privacy invasive, with who are they associated?
- From whom should the privacy invasive PzI pieces be withheld?
- What benefits are realised by withholding or not withholding privacy invasive PzI and in whose interests are the benefits?
- What are the motivations for users to disclose privacy to invasive PzI? And what motivators are present and in which kinds of personalisation?
- What additional privacy challenges are posed by personalisation in ubiquitous services and how are they mitigated?

### 2.4.3 Mitigation strategies

There are numerous privacy strategies to address aspects of the implications and threats of personalised services. These strategies can be distinguished as notice-based, policy-matching, cryptographic-approaches and privacy-frameworks. Notice-based approaches

present users with standardised symbols signifying that a specific service conforms to basic privacy. These symbols are termed privacy seals. Leading seal providers include TRUSTe and BBBOnLine [103]. Sealed services are billed an annual fee dependent on their yearly revenue and are promised a high return on seal investment. Prior to being sealed, a service must adjust its privacy disclaimer to the seal provider's standard and publicises it. Seal seeking services must also provide redress channels for complaints and opt-outs from direct marketing and third party PI disclosure. A drawback on seals is their lack of guarantee in PI handling rendering them as assurance mechanisms to inform consumers of the service following a particular privacy standard. LaRose et al. [86] points out that sealed services tend to request more privacy invasive PI from consumers than their unsealed counterpart. Furthermore, seal providers make no commitments regarding the levels of privacy offered by service bearing their seals.

Policy-matching approaches takes a further proactive step to minimising risk by enabling users to compose their privacy expectations and compare them with the service's privacy policies prior to service access. Privacy policies declare the service's intended use for requested PzI. Declarations comprise of collected data types, their permanence and visibility. Policy language implementations like Platform for Privacy Preferences (P3P) [36], Enterprise Privacy Authorisation Language (EPAL) [60], eXtensible Access Control Mark-up Language (XACML) [98] and Security Assertion Mark-up Language (SAML) [133] are XML based and support the definition, enforcement and obligation. The Privacy and Identity Management for Europe (PRIME) project extends P3P by availing technical means for processing PzI so that individuals retain sovereignty over its collection, disclosure and its obligatory use. XACML standardises access control and authentication in manners describing entities and their attributes while, SAML focuses on standardising the exchange of PI between identity provider and service provider [98, 133]. The fact that policy-matching approaches depend on the trustworthiness and regulatory pressure to ensure policy compliance behaviour implies it cannot enforce privacy.

Cryptographic approaches attempt to resolve privacy concerns by addressing the Confidentiality, Integrity and Authenticity (CIA) triad [128]. Confidentiality and integrity are straight forwardly attained with encryption and digital signatures but addressing availability or the complete triad is challenging due to additional needs for authenticity, authorisation, non-repudiation, access control, and accountability. Cryptography based detections like PRIVDAM [19] continuously monitor access to PI to detect abnormalities and then identify and penalise the violators. Pseudonymous [26], obfuscation [130, 152] and access control [108] are some prevention and control mechanisms limiting the misuse of PI by avoiding privacy critical operations or access.

Privacy-frameworks arise from novel combinations of cryptographic and policy-matching approaches. Beresford and Stajano [17] implement a privacy framework that conceals users current and/or past location from other parties by controlling access to their location data. In [17] users were identified using pseudonyms that change frequently concealing the user within the community as they visited pervasive locations. Beresford and Stajano adopt a mix zone concept as a measure of privacy level that allows users to opt-in to services providing anonymity set size of a given threshold, for instance, 20 users, which is deemed a sufficient guarantee assurance from pseudonyms link-ability [17]. The concept of anonymity set and the related formal protection model named $k$-anonymity was first proposed by Sweeney .L [87] study to deter re-identification attacks. In other

proposals, Könings et al. [79] incorporated ontology based privacy management and control framework into their Adaptive and Trusted Ambient eCOlogies (ATRACO) project. Privacy in ATRACO is addressed from informational P/GII, P/GPref and territorial (location, accompaniment) privacy perspectives ensuring sensitive PI is visible to owner's who control their revelation to others [79]. ATRACO adopts an interactive approach where service access is explicit and require users' approval.

Other proposals advocate privacy preservation through context management. For instance, context can be managed using knowledge networks to properly correlate and pre-digest context information so as to provide services with higher-level understanding of situations and reduce their burden [156].

Regardless of the adopted means of managing and controlling PI privacy adopted, privacy is a subjective matter and therefore replete with discrepancies. Subjectively, users evaluate similar PI items differently as to their privacy significance. *Jane* for example might consider her phone number personal and stringently safeguard it. *John* however might casually disclose his phone number. Privacy discrepancies are often observed when users' privacy decisions are compared with their attitudes towards privacy. Privacy economists term this, phenomena *Privacy Paradox* [113]. Inherently, assumed by the economists is that users seek to maximise their utility constantly by balancing costs and benefits of disclosed PI and receiving personalised services [12, 25].

## 2.5 Discussion

The study focuses on clarifying the manner by which users can access personalised ubiquitous services in privacy preserving mode. In accessing a local service, the user and service have similar S/CI attributes such as local time, current weather and location. In this instance, minimal benefits are derived in concealing these specific PzI from the service. The S/CI is implicit in accessing the service. In contrast, when accessing a remote service, the user's S/CI has more privacy relevance, and requires adequate protection.

Different combinations of PzI might be invasive if disclosed to a single service as with the combination of multiple weak identifiers. This invasiveness is amplified by multiple cooperating services to which users disclose different sets of PzI. If these distinct services compose unions, aggregations and intersections over the data sets, they are bound to defeat the implemented privacy strategies of disclosing to different services. The details of how a service handles users' PzI are thus important and have been discussed at length in [117, 119].

The PI users' disclose to services have different privacy implications depending on *who is asking* and *who makes the initial interaction*. For instance, in certain cultures, when the government asks for information, users are less inclined to disclose as compared to when corporations ask. The reverse is also true in other cultures. Frequently, users consider services to be more trustworthy if the user initiates the interaction. However, if the service does initiate the interaction, users regard them with greater suspicion. This is similar in principal to parents' advice to their young children not to talk to strangers. This advice misleads and discourages children seeking help from strangers when in trouble. Perhaps a better advice would be put as "do not talk to strangers who approach you first".

Chapter III

# Architecture

In this chapter, the architectural components of ME2.0 that enable users to disclose their PzI to ubiquitous services and receive personalised services in a privacy preserving manners are presented. Figure 3.1 provides an overview of the architectural composition and configuration of the infrastructure architecture and mobile terminal architecture.

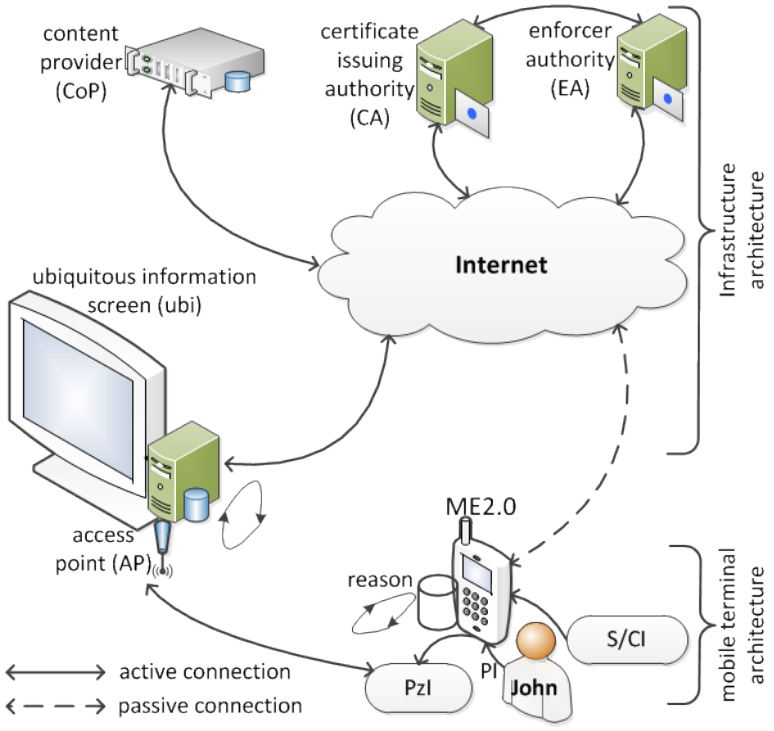



**Figure 3.1:** ME2.0 architectural overview.

The infrastructure architecture is the facilitating back-end system responsible for ensuring that services are trustworthy in the formulation and handling users' PI. Chapter 4 is concerned with the infrastructure architecture in the context of ME2.0 scenarios. The mobile terminal architecture that is responsible for sourcing, modelling, storing, reasoning and disclosing users' PzI to ubiquitous services. The interactions between the two architectures raise discussions on the privacy assurances and preservation mechanisms.

The usage of ME2.0 is envisioned to be mapped on top of the architecture to aid in elaborating the entities, their interactions, and to justify their inclusion. ME2.0 emphasises two personalisation scenarios with ubiquitous services; *Scenario-1* and *Scenario-2*.

***Scenario-1*** *Arriving at Helsinki Airport terminal 2, John has an hour to spare before boarding his flight to Tokyo, Japan. A nearby information screen begins to display content about Tokyo, its transport infrastructure, sites, weather, travellers' guides and so on. The display is split into four sections, while the main section focuses on Tokyo, the other sections display the latest ice-hockey results, a book review from John's favourite author and a trailer of Minority Report II.*

***Scenario-2*** *John arrives in Tokyo, after a long flight and plans to go to his hotel to freshen up. At the arrivals terminal, John notices the ubiquitous information screen displaying content personalised to his preferences, but he is not keen on publicly exposing his preferences. John configures ME2.0 and soon after list of restaurants serving Greek salad and Japanese vegetarian cuisines close by are sent to his mobile terminal non-interactively. The contents are automatically updated as his S/CI changes such as @restaurant or meeting postponed.*

Scenario-1 emphasises the personalisation of a publicly exposed information screen. The relevance of scenario-1 emerges where users intend to view generic and non-personal information that does not need to be concealed but preserves the leakage of their PI. Despite disclosing his PzI, John's personal privacy is left intact. This is because no identifiable PI, but rather the PzI are notated with his S/CI to disclose his CnP to the screen rendering the displayed content possibly relevant to other travellers as well. Scenario-2 situation depicts a setting where John prefers to have personalised content delivered to his mobile terminal. To realise the scenarios, different service types that may interact with ME2.0 should be considered. Additional to this consideration is the need to communicate reliably and efficiently. Communication should effectively convey the message, convenience the user and preserve privacy. Only authorised entities may communicate.

This chapter focuses on the mobile terminal architecture. The presentation takes a decomposition approach to systematically analyse the architecture into sub-components. The breakdown reveals design insights and eases the explanation of the sub-components with appropriate black boxes. A top-down approach enables the ME2.0 to be presented as a *black box* that focuses the initial attention to the service and communications tiers over the Open Systems Interconnection (OSI) model as Figure 3.2 depicts.

The service tier explains the mechanisms behind the functioning of different services accessed by users, their access implications with ME2.0 and their accompanying challenges. The challenges include engagements in data transformations (compression, decrypt/encrypt) that provide common interfaces and session management for ME2.0 and services interaction. The communications tier insulates the service tier from having to deal with

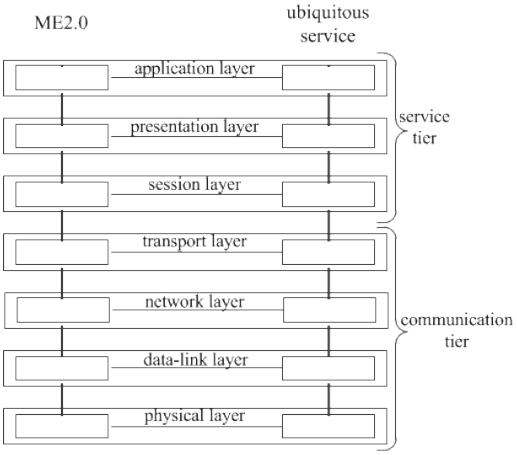



**Figure 3.2:** Service and communication tiers.

complexities of the transportation technologies such as reliability, error recovery or flow control that enable ME2.0 and ubiquitous services to interact.

## 3.1 Service tier

There are numerous services accessible to users from their mobile terminals. These services can be characterised on the basis of locality, communications, accessibility and interaction as depicted in Figure 3.3. Personal services are usually owned and accessed by a single individual in the confines of their personal spaces like home or work. When the service accessibility is specified to a fixed location or within given boundary constraints, it is considered a local service. Intranet websites and portals can be good examples of local services, if all the external and remote accesses are deterred. Other organisations might consider it beneficial to permit limited and strictly controlled access to their local services from externally located and authenticated users to access remote services. If access restrictions are removed allowing services to be made publicly available to all Internet connected terminal such as the WWW, they are considered an Internet located service.

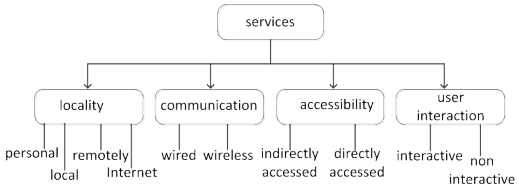



**Figure 3.3:** ME2.0 accessible service taxonomy.

ME2.0 communicates with services over wireless mediums facilitated by mobile terminal hardware. The depiction of wired communications in Figure 3.3 is only for clarification purposes.

ME2.0 was developed mainly for direct-access mechanisms between ME2.0 and services to disclose users PzI as depicted in Figure 3.4*(a)*, however other access manners are possible. In a direct-access ME2.0 utilises a Bluetooth communication network to interact with service. The interaction with services in direct-access manner can further be distinguished on the basis of the user interaction as interactive and non-interactively accessed services.

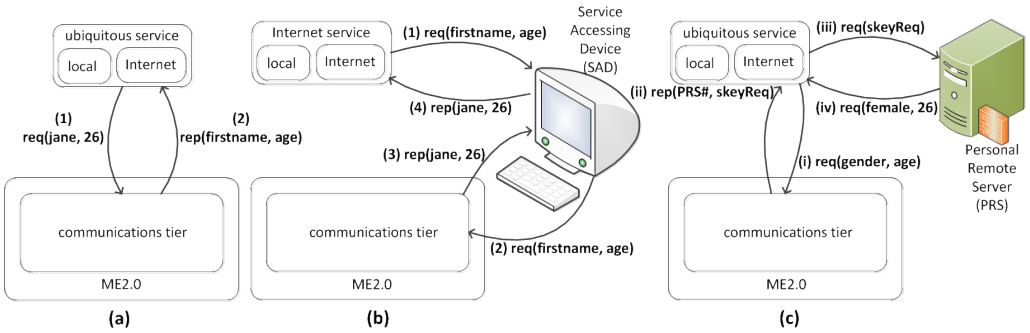



**Figure 3.4:** Accesses to services with ME2.0.

Interactive services demand explicit user involvement prior to accessing the service, such as John opting to decline or accept restaurant information from the information screen to his mobile terminal explicitly. Non-interactively accessed services are provided without the need for explicit involvement or action from the user. A GPS car navigation system constantly updates the car's location without the user directly accepting or declining all updates. Similarly, John's interaction with the information screen in scenario-1 is non-interactive.

The predominant service access manner used by ME2.0 is the direct-access characterised with non-interactive usage as this minimises amount of effort demanded from the user to access services. The transparency of the non-interactive access is emphasises ME2.0 capability to access service directly and automatically without manual entries from the user at access time.

Figure 3.4(b) depicts a secondary service access manner by ME2.0 through an intermediate terminal or application. The use of an intermediary terminal or application by ME2.0 to interact with services is an *indirect-access*. In the course of an indirect-access, ME2.0 provides PzI to an application executing on the intermediate terminal that actually accesses the Internet service. This intermediate terminal is termed a Service Accessing Device (SAD) and might be a desktop computer or another mobile terminal, while the application actually interacting with service is termed a Service Accessing Application (SAA). The indirect-access might also be with an application running locally on the user's mobile terminal like a web browser. ME2.0 might also interact with services in a direct-indirect manner as depicted in Figure 3.4*(c)*.

## 3.2 Communications tier

The communications tier facilitates ME2.0 interactions with ubiquitous services, SADs, service directories, Personal Remote Server (PRS) and EAs over various communication technologies as illustrated in Figure 3.5.

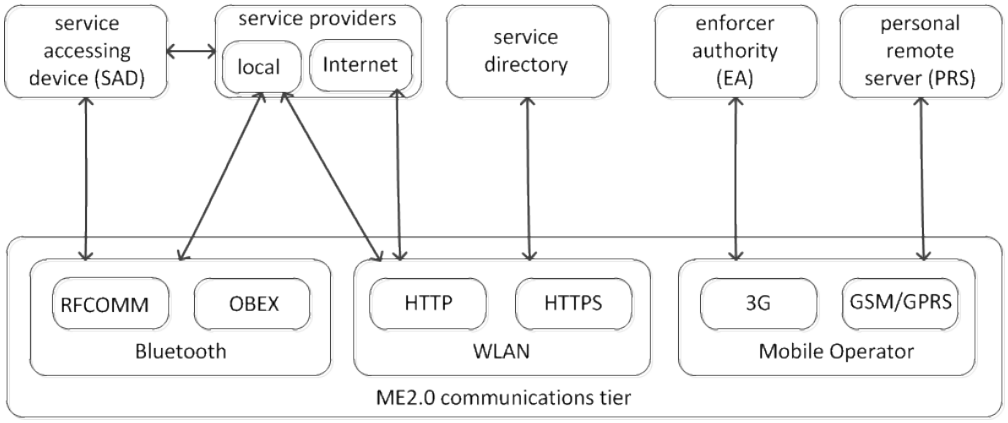



**Figure 3.5:** ME2.0 communication tier.

Services ME2.0 communicates with may be provided in public spaces such as the information screen at airports or malls. In using these services users PzI pieces stored in individuals' mobile terminals are transmitted by ME2.0 to the information screen with the intentions of viewing personalised content displayed on the public screen or delivered to the mobile terminals.

The communication technologies that enable the disclosure and delivery of personalised content are depicted in Figure 3.5 as Bluetooth [35], WLAN and mobile operator based. Internet based services, EA, PRSs and service directories are better accessed over WLAN and mobile operator networks. Local or close proximity based services like the ubiquitous information screen are suited to Bluetooth or WLAN mediums due to the fact that the user is close and can derive more benefits from visual cues [81].

In the direct ME2.0 and service interaction, Bluetooth is the preferred communication technology. Bluetooth is the propriety open wireless standard used by ME2.0 to access local proximity ubiquitous services due to its built-in Service Discovery Protocol (SDP). Additionally, Bluetooth has an implied reliability feature derived from its Frequency Hopping Spread Spectrum (FHSS) that slightly complicates eavesdropping and jamming efforts. Bluetooth is predominant in most mobile terminals today, thereby allowing ME2.0 to function in heterogeneous devices.

There are communication similarities in accessing Internet based services with ME2.0 and through the SAD as Figure 3.5 depicts. The similarities are in the appearance of the service to ME2.0 communications tier and the SAD to the communications tier. Negotiations and disclosures of PI are similar in both interactions. ME2.0 does not communicate directly with the Content Provider (CoP). All CoP communications are

conducted by the service provider in retrieving relevant content based on disclosed PzI. The role of EA is to verify the credentials of service providers and investigate their misconduct. There are benefits in encrypting communication between ME2.0, EA and PRS. Communications over WLAN are suitable for querying the list of services. The communications between ME2.0 and remote services of EA and PRS are implemented in a Service Oriented Architecture (SOA) manner using Remote Procedure Calls (RPC) over Hypertext Transfer Protocol Secure (HTTPS).

Operator mobile communication technologies are used minimally in ME2.0 communications as they often have financial implications for their owners in comparison to Bluetooth communication. In interactions, between ME2.0 and the EA or the PRS, the transmitted data should not be visible to the service operators plain text.

### 3.2.1 Communications format

All communications between services and ME2.0 are formatted in XML to enable encoding the various interaction meta-data in formats portable across heterogeneous mobile terminals. To parse and retrieve meta-data content from the ME2.0 XML communications, an XML-Parser is used to convert the meta-data into XML-DOM. This makes it easy to manipulate messages with minimal storage requirements.

Formatting ME2.0 communications in XML renders the appropriate data transfers protocols for Bluetooth communicating services and ME2.0 as Radio Frequency Communications (RFCOMM) over Object Exchange (OBEX) (Figure 3.5) RFCOMM provides a simple reliable data stream that is similar to Transmission Control Protocol (TCP) at the protocol level that does not overload the Bluetooth protocols. This implies that the communicated XML documents are first read in as a string then transmitted as bits of data.

Formatting communications between ME2.0 and ubiquitous services means that their messages follow the right arrangement of data. However it does not imply that the content of the data is meaningful. Rendering the content meaningful is the role of notation. Requests from the service have to be notated in a manner that ME2.0 in the mobile terminal can understand and respond to. Similarly, responses from ME2.0 have to clearly demarcate the PzI they disclose. Otherwise services would not be able to provide the intended personalisation.

To notate communications, ME2.0 utilises ME2.0 Modelling Language (ME2ML), a naming concept based on Electronic Commerce Modelling Language (ECML) [39] but adapted for applicability in the domain and inclusion of P/GPref, S/CI and their defining attributes (Appendix I). ECML was developed to standardise the notation of information on-line retailers request from their customers in terms of naming conventions, structure and layout of checkout forms.

Digital wallets and E-commerce services such as Windows Live ID (formerly Microsoft .NET passport) and wallet utilise ECML [92]. Microsoft's .NET passport provided authentication services while the wallet stores users' personal and financial information at Microsoft's servers enabling them to conduct purchases without re-entering these credentials each time. Privacy concerns on the collection and storage users' information on Microsoft's servers and interoperability with other solutions such as Liberty Alliance

led to the unpopularity and subsequent repositioning of .NET passport and wallet as Windows Live ID.

An important part of ME2.0 communications is the ability to provide sufficient and verifiable service credentials to users, while retaining the control of what PI users disclose. This can be attained by enabling the manners in which users can ascertain service credentials by first enlisting the services from a service directory. Enlistments from the service directory binds the service credentials to the users ME2.0 instance as depicted in Listing 3.1.

**Listing 3.1:** A *meRequest* excerpt

```
<me_request>
  <credential>
        <serviceName>aiportUbiScreen</serviceName>
        <sphere>community</sphere>
        <valid>10:49:56 09.11.2011 GMT</valid>
        <category>informative</category>
        <description>personalised informative screen</description>
        <owner>andrew thorton</owner>
        <bdaddr>00:10:60:D2:A1:4C</bdaddr>
        <ciphers>
              <ecc>
                 <parameters>NID_sec233k1</parameters>
                 <cipherKey>-----BEGIN PUBLIC KEY-----
                    MFdfg5IWgdhgEAYHghfkfKOZL1fghloh2L1zxcvweFG
                    -----END PUBLIC KEY-----
                 </cipherKey>
                 <signKey>-----BEGIN PUBLIC KEY-----
                    eSDFGSDrsdfgDF345SD567FG8JKGGdfgdfSMsdfg
                    -----END PUBLIC KEY-----
                 </signKey>
              </ecc>
              <x509>
                  <certifier>https://ca.context.h1x.com:8444</certifier>
                  <sign>signature</sign>
              </x509>
              <ea>
                  <enforcer>htpps://ea.context.h1x.com:8445</enforcer>
                  <sign>signature</sign>
              </ea>
        </ciphers>
  </credential>
  <request>
    <item>me_preferences_news</item>
    <aim>inform</aim>
    <kept>6</kept>
    <oblige>false</oblige>
    <seclev>restricted</seclev>
    <share>eMeal</share>
  </request>
</me_request>
```

The response from ME2.0 instance *meReply* to verified credentials is based on the XML schema defined in Appendix I.2 to include the user's PzI disclosures as illustrated in Listing 3.2. In contrast to *meRequest*, the *meReply* is compacted by removing irrelevant data, sometimes compressed and always encrypted. The *meReply* contains disclosed PzI

notated with the users S/CI to compose their CnP. Accompanying the *meReply* are notations of users privacy expectations.

**Listing 3.2:** A *meReply* excerpt

```
<me_reply>
  <credential>
        <serviceName>aiportUbiScreen</serviceName>
        <ciphers>
              <ecc>
                 <parameters>NID_sec233k1</parameters>
                 <cipherkey>-----BEGIN PUBLIC KEY-----
                   23aASDd4MasdADSFfasOZL1asADdfgdSDfzxASD
                   -----END PUBLIC KEY-----
                 </cipherkey>
              </ecc>
        </ciphers>
  </credential>
  <reply>
    <me_preferences_news>nhl ice hockey</me_preferences_news>
    <me_preferences_language>english</me_preferences_language>
  </reply>
</me_reply>
```

To make it easy to save and retrieve matching PzI from the mobile terminal's databases, there is a direct mapping of ME2ML naming conventions to the database tables.

## 3.3 ME2.0 and PzI

The different types services to which ME2.0 may disclose users' PzI have been presented in Section 3.1. Disclosures of PzI to these services also utilise different underlying technologies for the transfer as discussed in Section 3.2. This section takes the discussion further by detailing how the PzI arrives at ME2.0.

Individuals executing ME2.0 in a mobile terminals they frequently carry and use, expose their PI items, their experiences and situations to ME2.0. The exposure comes about in the course of daily activities and mobile terminal use as the individuals add, remove, and modify information items on their mobile terminal. Some of these modifications might be intentional and planned while others may be spontaneous and unplanned. Changing the mobile terminal's profile to silent/flight mode before boarding a plane or setting the alarm for the next morning are planned activities. However, updating weather, news or Twitter feeds are often unplanned and in some cases automated.

There are two primary ways in which PzI arrives at ME2.0, *user-input* and *inferred-input*. Aggregating these primary manners implies four solicitation channels:

- **User sourced** - PzI sourced directly from the user by selecting UI widget component like drop-down or check-box item or by typing in values like names, age, preferred meals.
- **Sensor source** - Terminals internal or external accessible sensors. Internal sensors inference on orientations, location and proximity.

- **Terminal sourced** - Configurations, status and utility programs providing terminals defaults like language, active profile and notifications.

- **SAA** - Applications accessing services of other providers like E-mails exchanges, web services and social networks clients.

Individually, the information pieces do not amount to much. However, combinations, corrections, updates, aggregations and further refinements transform the items into abundant PI. The PI abundance can be selectively used as a PzI disclosure to ubiquitous services by ME2.0 on behalf of the users.

### 3.3.1 User entries

ME2.0 cannot know any intricate PI detail of its hosts such as gender, age and meal allergies, unless they are explicitly entered. This is also the case with details of P/GII, SI and P/GPref. Some NP/GII and contactable information are also included in this category. To use these PI in ME2.0 for composing PzI that are disclosed to ubiquitous services, the user has to manually input them beforehand. ME2.0 classifies these PI items as Table 2.1 depicts, in order to maintain ME2ML notation for later compatibilities and storage convenience in the terminal's database.

The most used user controls to collect the PI items in Table 3.1 are text-input, number-input, dates and drop-down selections. ME2.0 aims at easing the inputting of these PI items through implemented structural organisations of personal, work, home, e-society and payments as depicted in Table 3.1. The structural organisation is used to compose the ME2.0 menu with the information they solicit taken from the naming conventions suffix. For example, a personal menu will have fields for the user to input their firstname, lastname, gender, birthplace and so on

Similar to the personal menu (Table 3.1), P/GPref is solicited under the menu preferences as depicted in Table 3.2. However, unlike the personal menu the dominant preference user controls is the drop-down selection to limit the potentially infinite options of users to the closest matching preference.

The advantage of user entered information into ME2.0 is that the information about the users is likely to be more accurate and relevant compared to inferred information. Take for example that a user's default language in the mobile terminal is *English*. This language, however might be different from the preferred language, which might be *Finnish*. Explicit user input to a PI rather than inference also gives a comprehension of PI that might be exposed. This comprehension affords the users the opportunity to adjust the granularity or accuracy of their inputs. The adjustments accords users some form of privacy.

In spite of the direct user entry advantages, the process also has some limitation. Direct entry into mobile terminals is prone to errors from the terminal's limited ergonomics of compact keyboards and miniaturised displays. Entering or updating the information a number of times can be cumbersome for users. The fact that the user has to divert his attention from other tasks and concentrate on entering information into the mobile terminal is itself distractive.

**Table 3.1:** ME2.0 user input classification and naming.

| Menus | Items naming conventions |
|---|---|
| personal | me_data_firstname, me_data_lastname, me_data_nickname, me_data_birthplace_zip, me_data_middlename, me_data_gender, me_data_birthdate_day, me_data_birthplace_city, me_data_birthdate_month, me_data_birthdate_year, me_data_birthplace_country, me_data_birthdate_birthstreet1, me_data_birthplace_birthstreet2, me_data_birthplace_birthstreet3 |
| work | me_contact_email_work, me_contact_email_main, me_contact_email_alt, me_contact_email_trash, me_contact_phone_work, me_contact_address_street1_work, me_contact_street2_work, me_contact_address_street3_work, me_contact_address_city_work, me_contact_address_state_work, me_contact_address_country_work |
| home | me_contact_phone_home, me_contact_phone_cell, me_contact_address_street1_home, me_contact_address_street2_home, me_contact_address_street3_home, me_contact_address_city_home, me_contact_address_zip_home, me_contact_address_state_home, me_contact_address_country_home, me_contact_address_street1_alt, me_contact_address_street2_alt, me_contact_address_street3_alt, me_contact_address_city_alt, me_contact_address_zip_alt, me_contact_address_state_alt, me_contact_address_country_alt |
| e-society | me_contact_irc, me_contract_forum, me_contact_website, me_contact_blog, me_sns_twitter_url, me_sns_facebook_url, me_sns_other_url |
| payment | me_payment_card_type, me_payment_card_name, me_payment_card_number, me_payment_paypal, me_payment_card_verfication, me_payment_card_issueNumber, me_payment_from_date, me_payment_expire_date |

### 3.3.2 Inferred entries

Many terminals today have an array of in-built sensors and various mechanisms to access external data. Popular in-built sensors include GPS receivers, accelerometers, ambient-light, noise, touch, proximity and orientations sensors. Access to external sensors is facilitated by communication technologies like Wi-Fi and Bluetooth. ME2.0 delegates the responsibility of gathering sensor information to the sensor-engine (see Figure 3.6). The sensor-engine is also responsible for ensuring the correctness and storage of the sensor data.

The sensor-engine in ME2.0 uses the *inquisitor*, an ME2.0 helper application that routinely reads sensor data at predetermined time intervals. In ME2.0, a default time interval is set at 30 minutes, so as to preserve the terminals battery and provide distinguishable sensor readings. The current version of the inquisitor obtains reading of operator cellular towers, GPS details (like satellites, location, direction, speed), nearby Bluetooth devices,

**Table 3.2:** ME2.0 P/GPref naming and selection alternatives.

| Preference | Options |
|---|---|
| me_preference_news | weather, stocks, bbc, cnn, yle |
| me_preference_sports | hockey, ice-hockey, soccer, tennis, rugby, volleyball, basketball |
| me_preference_music | classical, jazz, rap, heavy, rock, RnB |
| me_preference_language | English, Finnish, Swedish, German, French |
| me_preference_meal | cafe, Italian, vegetarian, Chinese, kebab, Pizza, Greek, Irish |
| me_preference_film | sci-fi, romantic, action, horror |
| me_preference_shop | art, antiques, real estates, jewellery, mall |
| me_preference_restaurant | Indian, Nepalese, English, Fast food, Take away, Coffee shop, French |
| me_preference_beverage | lemonade, beer, cider, fizzy drink, vodka, coffee, tea, juice |
| me_preference_vacation | Caribbean, hiking, water sport, sunny island, exotic island, massage, yoga, prehistoric |

pervading Access Point (AP)s, accelerometer and orientation readings. The sensor readings are time stamped and stored in a sensor database in ME2.0.

Other ME2.0 inferred entries are the terminal settings, configurations and status. After obtaining a new mobile terminal, most users personalise and configure their mobile terminal's alerts, UI layout, ring tones, ring levels, ring type, background colours, wall papers and language. Regardless of how trivial these alterations are, they provide invaluable insights into user's preferences. For example, user defined battery warnings can act as triggers disabling or adjust the inquisitor's intervals.

Mobile terminal's programs like alarms, to-do lists, reminders, calendars, E-mail clients, weather and SN widgets enrich the ME2.0 situation characterisation by providing details of user situations. The alarm clock gives a view of how the user organises their time and import events they would rather not miss. Similarly, SN widgets can provide a wealth of inferences for users' on-line activities. To make inferences on some SAA like SN widgets, the users need to disclose their access credentials to ME2.0.

## 3.4 ME2.0 internal components

The internal components of ME2.0 are important to comprehend the advantages and limitations of PI sources available to ME2.0 and for disclosing to ubiquitous services and accessing personalised services. Figure 3.6 illustrates the internal components of the ME2.0 architecture.

PI pieces in ME2.0 have bearings on how they are accessed, when they accessed, how they are stored and their privacy implications. The initial *meRequest* is transmitted from a ubiquitous service ⓐ to an ME2.0 as a solicitation for PzI. The solicitation is required in

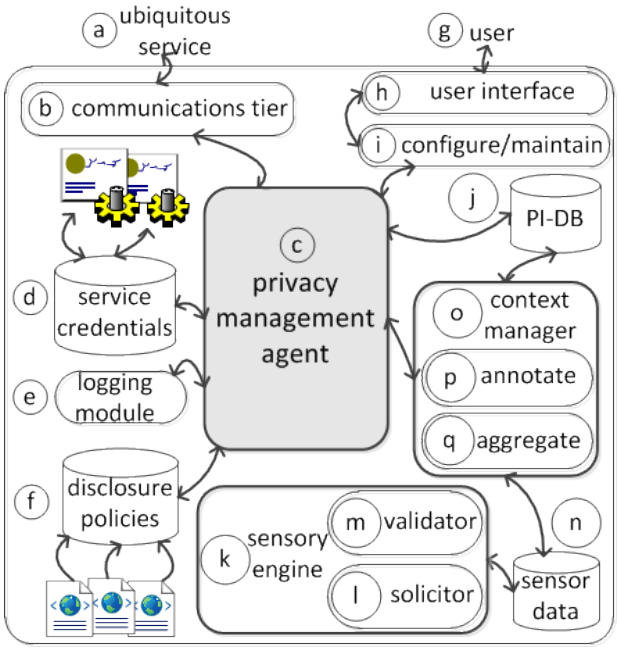



**Figure 3.6:** ME2.0 internal components.

order for the service to personalise its offers. This transmission involves a communications interface in the *communications tier* ⓑ. The *meRequest* is the culmination of the service's credentials, solicited PzI and its privacy policy into an XML document of the format depicted in Listing 3.1. The communications interface relays this *meRequest* to the privacy management agent ⓒ.

The privacy management agent is responsible for verifying the authenticity of a service against enlisted service credentials ⓓ. If the service had not been previously enlisted, it is marked as unverified (grey-listed) in the credentials database. The verification process and its decision are all logged by logging module ⓔ. Grey-listing may results in the termination of all interactions involving ME2.0 and the service unless explicitly overridden by the user. For verified service credentials the process continues with the privacy management agent matching the service's privacy policy and PzI requests against predefined disclosure policies stored at ⓕ. Matches between the service's privacy policy, its PzI request and ME2.0 disclosure policies are attended to while mismatches are ignored.

All ME2.0 settings enabling the acceptance of ubiquitous service *meRequest* for PzI and the composition of users' disclosure policies for *meReply* is accomplished by the user ⓖ via the UI ⓗ.The mapping of users disclosure policies to the database renders the evaluation and comparison with services *meRequest* to be conducted as SQL syntax statements. The users also configure and maintain in ⓘ their PI items, their preferences, their disclosures exceptions, their S/CI and sensor settings. Configurations involving inputting of PI are stored in the PI-DB ⓙ, while those involved with sensor readings are stored in the sensor database ⓝ. In configuring their privacy settings, users determine what information items are stored in cipher and plain text in the PI-DB and sensor

databases.

The ME2.0 sensor engine ⓚ is composed of a solicitor ⓛ and validator ⓜ agents. The solicitor is responsible for obtaining permitted sensor readings from the terminal's internal and external sensors, then storing them to the sensor database ⓝ. Sensor readings are often erroneous and inaccurate due to the diversity of their formats. It is the role of the validator ⓜ to go through sensor information stored in the database and validate their entries as well to delete or purge stale or incomplete database entries. The context manager ⓞ uses the sensor and PI-DB databases along with the privacy management agent setting to aggregate ⓠ and annotate ⓟ items when formulating the CnP to be disclosed.

### 3.4.1 Privacy management agent

The privacy management agent determines which enlisted services may request PzI from ME2.0. Users enlist services from a service directory or on the fly upon discovering the service. The benefit of service directory enlisting is the immediate verification of the service's authenticity and accessing of personalised. On the fly service enlisting postpones the authenticity checks for later access to the service directory. Prior to enlisting services, comparisons are made based on their PzI requests with those the users is willing to disclose, as well as how the service intends to processes the users PzI.

Relevant attributes relevant in the comparison are depicted in Listing 3.3, the *meRequest* schema excerpt as $item, aim, kept, oblige, seclev$ and $share$. The solicited PzI is represented by the *item*. The aim specifies the motive behind the information request by the service and may take various values such as inform, filter or contact. The *kept* attribute determines the PI permanence expressed as non-negative positive number of hours from 0.

The *oblige* attribute takes on boolean values to inform ME2.0 whether a particular PzI item is mandatory for disclosure or optional to provide the service. Value $oblige = false$ indicates that the PzI item is optional (service enhancement), while $oblige = true$ indicates it is mandated (service facilitation). For example, the meal locator implements this feature by requiring users to be above 18 years of age before recommending beverages/meals in bar or pub restaurants. This age requirement might also be affected by the S/CI of the user's location, so that in Germany it would be 16 years of age and 21 year in the United States.

**Listing 3.3:** Privacy attributes of meRequest excerpt

```
<xs:element name="request" minOccurs="1" maxOccurs="unbounded">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="item" type="xs:string"/>
            <xs:element name="aim" type="xs:string"/>
            <xs:element name="kept" type="xs:nonNegativeInteger"/>
            <xs:element name="oblige" type="xs:boolean"/>
            <xs:element name="seclev">
              <xs:restriction base="xs:string">
                <xs:enumeration value="public"/>
                <xs:enumeration value="restricted"/>
                <xs:enumeration value="confidential"/>
                <xs:enumeration value="secret"/>
                <xs:enumeration value="top_secret"/>
              </xs:restriction>
            </xs:element>
            <xs:element name="share" type="xs:string" minOccurs="0"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
```

The *seclev* is inspired by the military security policy [128] and in particular its formalisation by Bell et al. [14] confidentiality model. The *seclev* determines allowable communication when confidentiality needs to be maintained. The five levels, ranging from 0 to 4, as defined in ME2.0 coincide with public, restricted, confidential, secret and top-secret classification of PzI. The clearance levels are assigned to services by users for specific information pieces depending on the sensitivity of information solicited and the expected service. The police might be given clearance on certain PzI like identity and address, but not on medical details. Associated *seclev* also have implication on the adopted encryptions standards, such that $seclev = 0$, less stringent encryption compared to $seclev = 4$. The encryption robustness, are negotiated between ME2.0 and services such that the greatest common *seclev* is adopted by ME2.0 rendering PzI requiring more stringent confidentiality undisclosed. Thus, different information pieces may be protected at different security levels, for example $seclev = 4$ for medical details and $seclev = 0$ for musical preferences.

The *share* attribute is concerned with third party disclosures the service wishes share with. The share attribute takes a list of permitted service domains (such as advertisements, entertainment, education or healthcare) or an individual service (ubiquitous information screen). The privacy management agent also examines the *meRequest* validity, its digest and EA address. These examinations aim to mitigate falsified service credentials. The service name might be easily duplicated; therefore the EA detects and denies the registration. Adversaries armed with fake credentials are also unable to decrypt the response from users.

The ME2.0 encryption is implemented with Elliptic Curve Cryptography (ECC) [62]. Selection of the ECC public-key cryptography is on merits in offering equivalent security as traditional systems but with smaller key sizes [20, 59]. The smaller key size implies faster computations, lower power consumption, less memory and bandwidth usage, which are attractive for mobile terminals and ubiquitous communications. A service *meRequest* is an EA concatenation of PzI being solicited (*sports and music*), the services public-key,

and its ECC domain parameters to ME2.0 as Figure 3.7 illustrates.

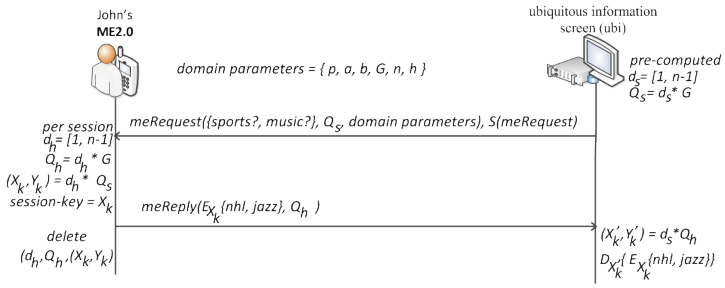



**Figure 3.7:** ME2.0 key-exchange and *meReply* encryption.

Figure 3.7 incorporates the Elliptic Curve Diffie-Hellman (ECDH) key-exchange in the communication between the information screen and John's ME2.0 formulates a shared symmetric-key ($X_k$). While the information screen's public-key ($Q_s$) is unchanged for duration of the service's policy validity, John's public-key ($Q_h$) is recomputed for each session thereby resulting to always different session-keys for symmetric encryption and decryption of PzI disclosures to the screen and services. Therefore, while an attacker might be able to replay John's *meReply* they have no means of associating the previous *meReply* from John. The changing of John's public-key and not the service's hinges on the fact that John need to authenticate the service and not the other way round. The service only needs to verify the integrity of the response from John which is accomplished by verifying $hash(E_{X_k}(nhl, jazz))$. The combination limits an attacker from decrypting $E_{X_k}(nhl, jazz)$ as they have no means to determine $d_h$ or $d_s$.

### 3.4.2 Modelling and storing

After sourcing PI items from various channels into ME2.0, they are modelled and stored in a manner that retains the modelling principles. In the modelling stage some PI items may be aggregated and others are fused. ME2.0 adopts a hybrid modelling approach that combines XML, databases and OWL-DL ontologies. The latter two are used to model relationships and dependencies between attributes and situations. The relational database inspired models are used for actual data referencing by the mark-ups and ontology models.

Some PI items have greater privacy requirements than others, and so require additional safeguards. Other PI pieces also have greater dependencies and relationships. Maintaining these dependencies and relationships require different storage mechanisms. Stored along with these PI items are their dependencies, relationships and determinants.

The access and usage needs of sourced and modelled PI items affects their representation and storage in ME2.0. The need to cater for heterogeneous services also implies that these formats should be portable despite their stored environments.

Three storage options used to store PI pieces in ME2.0 are key-value stores, relational databases and XML files. Stored PI pieces have quality requirements that determine how fresh or how frequent they are updated. Quality requirements place the burden of

the accuracy of the information on how frequently it is considered stale and therefore updated.

The use of stored PzI has two possibilities. Firstly, the entire PzI collection may be disclosed to ubiquitous services which will then process it to return the personalised service. Secondly, usage of the PzI within the device itself to consider the most suitable service behaviour disclosing only their CnPs. The PzI for disclosure or share outside the mobile terminal are converted into XML formats to enable portability.

Storing all PzI in the device memory is bound to have performance implications for the user. Therefore, depending on some accuracy-performance trade-off of the PzI stored in memory. PzI retention also determines an important factor affecting the device storage. Constantly added or archiving PzI also piles up and exhaust the devices storage, hence after some predetermined duration, the PzI should be purged or backed-up outside the device (PRS).

The ME2.0 storage uses three database implementations of e32db, e32dbm and SQLite3 depending on the mobile terminal environment on which it executes. The e32db and e32dbm are defined for Symbian OS in Nokia Series 60 [110, 111]. The e32db implementation supports transactions and querying using SQL to organise data in a relational manner similar to SQLite3 [111, 141]. In contrast, e32dbm adopts a dictionary based approach that stores data in key-value pairs [111]. SQLite3 is often marketed as *"a software library that implements a self-contained, server-less, zero-configuration, transactional SQL database engine"*. SQLite3 is a lightweight and portable database used in ME2.0 implementations on Linux based terminals like Nokia N770, N810 and N900 [141].

The four databases in ME2.0 implementation illustrated in Figure 3.6 are used to store service credentials, users' disclosure policies, sensor data and PI pieces. The sensor database is implemented using e32db module while the PI-DB implementation is based on e32dbm modules. The disclosure policies and service credentials database are XML documents mapped into e32db with each single row representing an individual file extraction. The rationale for selecting one database over another is the amount of information to be stored, the importance of that information to ME2.0 and mobile terminal OS.

## 3.5 Discussion

Chapter 3 has presented the overall architecture for the ME2.0. The details of the architectural components are discussed with examples of their functionalities. ME2.0 mechanisms enabling the determination, processing, storage and disclosure PzI by users as well as, the notation of PzI and with S/CI to attain CnP are also presented.

Mechanisms preserving the privacy of PzI during context storage, processing and disclosure to services in order to access personalisation services are demonstrated. The privacy perspectives are addressed in relation to modelling of the sourced information, storing the information and users' privacy expectations to limit disclosures under certain conditions. The ME2.0 architecture thus, provides answers to the questions on users' control, notification and consent of disclosed PI. Articulating differences in expected privacy, alternative disclosures, PI confidentiality, disclosures accountability and services authentication is needed to give assurance to users.

Nonetheless, avenues for further research exist with ME2.0 to address recent advances in *cloud computing* architectures. Such architectures would for instance have effect on the communication model depicted in Figure 3.4 permitting additional communication with services and other terminals over the 'cloud' even if they are in close proximity.

Chapter IV

# ME2.0 and services

This chapter presents a discussion of how users can feasibly access personalised ubiquitous services using ME2.0 with less vulnerability and potential invasion of their privacy in different scenarios. The sequence of steps in ME2.0 use is:

1. User starts ME2.0 - user authentication.
2. Access requests for ME2.0 data from services - service authentication.
3. Determine the data to disclose - service verification.
4. Securely transmit data to the right service - disclosure.
5. Receive content tailored to the user - service personalisation.

## 4.1 Authentication

The definition of authentication found in the IS0 7498-2 [69] standard has been widely adopted an is in wide use. The standard defines authentication to comprise two parts: *entity* and *origin*. The *"corroboration to one entity that another entity is as claimed"* is provided by entity authentication and might take place during a connection establishment to mitigate masquerading or replay attacks. *"Origin authentication provides corroboration to an entity that the source of received data is as claimed"* without guarantees of its duplication or modification. [69]

Schneier [137] elaborates that with authentication, *"it should be impossible for intruders to masquerade as someone else"*. In this study, authentication is discussed in terms of confirming the presented credential claim by a user, ME2.0 and services. In this respect, these are not mutual authentication rather interactions upon which an entity conducts a one-way authentication to another in:

- User to ME2.0 authentication.

- Service to ME2.0 authentication.

Mandating authentication on these interactions increases the robustness of the privacy preservation mechanisms at the expense of performance and usability, thus, trade-offs has to be considered.

### 4.1.1 User authentication to ME2.0

A process for a user to authenticate himself to to the ME2.0 instance that discloses their PzI to ubiquitous services is required when configuring ME2.0. User authentication to the mobile terminal is initialised by authentication to the terminals Subscriber Identity Module (SIM) by providing a correct Personal Identification Number (PIN). The SIM is an integrated circuit storing International Mobile Subscriber Identity (IMSI) and other keys used to identify and authenticate subscriber on mobile terminals.

The authentication step involving the user authenticating themselves to ME2.0 is important. The importance arise from the need to ascertain that the PI disclosed was actually created by the user accessing and configuring ME2.0 whether or not it truly reflects his personality. This authentication to ME2.0 may be based on some relevant factor which is inherent to the user or his knowledge of an authentication factor. Authentication system employing inherent factors are likely to be based on biometrics in mobile terminals. Knowledge factored authentication schemes are based on something the user knows such as passwords, PIN codes or pass-phrase [128].

Unfortunately, each of these authentication mechanisms has its circumventing limitations. Fake biometric injections, covert acquisitions and replay attack circumvent the inherent factored authentication schemes. Knowledge factored authentication employs secrets that users stores in their minds. Overtime even the mind is weak against interrogative methods (rubber hosing) designed to reveal these secrets. Additionally, weak passwords are predictably brute forced or dictionary attacked, strong passwords difficult to remember and frequently changed passwords easily forgotten leading to password fatigue [95].

User authentication to ME2.0 implements the traditional user-name / password pair and a challenge-response second level authentication from pre-input PzI. In addition, S/CI is incorporated to distinguish user authorisation in different setting. For instance, in the safety of their home or work, a logged-in user has greater authority to make higher access-level changes to ME2.0. However, in a public place authorisation is constrained. The user-name in ME2.0 authentication is the user's registration E-mail address as the initial ME2.0 credentials and the password is an alpha-numerical code. The incorrect entry of the user-name / password pair three times locks ME2.0. The ME2.0 password recovery mechanism sends a randomly generated password to the user's registration E-mail address. Recovered passwords are re-generated as ME2.0 stores passwords as MD5 digests. The challenge-response is based on the random choices of PzI entered by the user such as favourite musician, meal and so on.

### 4.1.2 ME2.0 authenticating Services

The purpose of ME2.0 is to transfer PzI to ubiquitous services automatically and securely based on owners' privacy expectations. Whilst trusted services receive more PzI, services

upon which the user has no prior interactions are also supported but, accorded less users' PzI. This implies that ME2.0 needs to authenticate services to disclose more PzI. Automation concerns the transfer of PzI without the user's explicit authentication for service disclosure. The privacy expectations base the decision solely on previously entered user PzI. The authentication of services by ME2.0 is unobtrusive. Service authentication to ME2.0 relies principally on ME2.0 authenticating the service and not the other way around.

Services that interact with ME2.0 include their authentication credentials in their request (*meRequest*) enforced policy as Listing 4.1 depicts. Credentials of interest are the Bluetooth Device Address (*bdaddr*), cryptographic materials (*ecc*) and certificate. The Certificate Issuing Authority (CA) has already verified the association of these credentials to the named service with their signature. Through the EA and service directory ME2.0 also has access to this information. The *bdaddr* is an optional attribute for the authorisation authority in a delegated multi-site service scenario as depicted in Figure 4.1.

**Listing 4.1:** Authenticating credential in a *meRequest* excerpt

```
<serviceName>aiportUbiScreen</serviceName>
<sphere>community</sphere>
<valid>10:49:56 09.11.2011 GMT</valid>
<category>informative</category>
<description>personalised informative screen</description>
<owner>andrew thorton</owner>
<bdaddr>00:10:60:D2:A1:4C</bdaddr>
<ciphers>
      <ecc>
        <parameters>NID_sec233k1</parameters>
        <cipherKey>-----BEGIN PUBLIC KEY-----
          MFdfg5IWgdhgEAYHghfkfKOZL1fghloh2L1zxcvweFG
          -----END PUBLIC KEY-----
        </cipherKey>
        <signKey>-----BEGIN PUBLIC KEY-----
          eSDFGSDrsdfgDF345SD567FG8JKGGdfgdfSMsdfg
          -----END PUBLIC KEY-----
        </signKey>
      </ecc>
      <ca>
          <certifier>https://ca.context.h1x.com:8444</certifier>
          <sign>signature</sign>
      </ca>
      <ea>
          <enforcer>htpps://ea.context.h1x.com:8445</enforcer>
          <sign>signature</sign>
      </ea>
```

In a single service deployment, the service requests PzI by sending its *meRequest* to ME2.0. On encountering the request for the first time, ME2.0 verifies and double-checks its integrity by verifying the CA signature. If these integrity checks are successful, the *bdaddr* from which the request originates is compared to that in the credentials. If these match, then the service is considered authenticated and its cipher-key safe to formulate the shared symmetric-key. In addition, placing the user in control of disclosed PzI enables them to control service authentication strictness by adjusting the *seclev* attribute permitting "on-the-fly" service authentication that does not require immediate EA au-

thentication rather only the CA in a manner similar in implementation to web browsers and root certificates.

In a multiple service deployment, consider a restaurant franchise with subsidiary restaurants nationwide. If the franchise head office decides to deploy ubiquitous information screens at its headquarters $hq$, regional $r1$, and local $l1$ restaurants as Figure 4.1 depicts. Then a customer visiting different subsidiaries and keen to receive personalised services from their screens would be required to install each restaurants' enforced policy and authenticate each restaurant individually. This approach suffers from the "flawed assumptions" of a global directory and that directory names are usable securely in centralised Public-Key Infrastructure (PKI) [41].

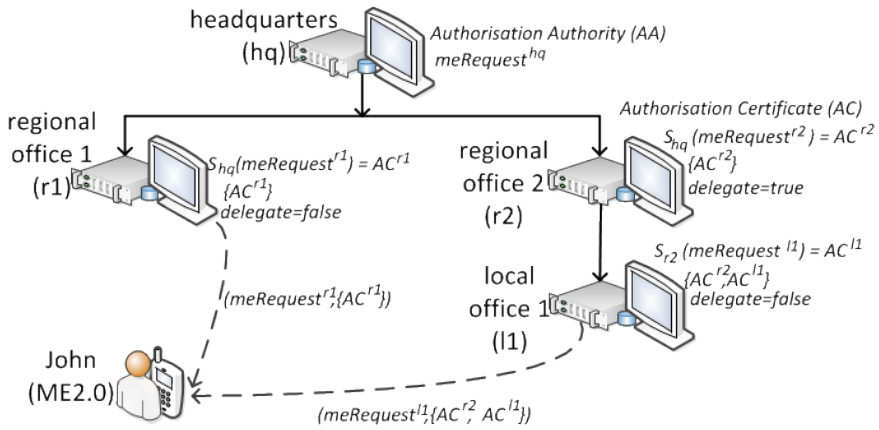



**Figure 4.1:** Delegated service authentication and authorisation.

However, if $hq$ assumes the role of an Authorisation Authority (AA) issuing Authorisation Certificate (AC) to its subsidiary in a chained manner, it minimise customers' frustrations, storage and communications to authenticate the subsidiary. The concepts of AA and AC originate from Ellison's [40] proposed Simple Public-Key Infrastructure (SPKI), an access control scheme with public-key focused on naming of identity [41]. The SPKI defines an AC in particular to comprise five elements: (i) an issuer $I$ that created and signed it; (ii) a subject $S$ to whom it is issued or delegated; (iii) a delegation element $D$ specifying whether the subject can further delegate the authority in the AC to third parties; (iv) an authorisation $A$ the extent of the AC's authority; and (v) time period for AC's validity $V$, denoted as $AC = \{I, S, D, A, V\}$ [42].

The $hq$'s enforced policy or $meRequest$ is proof of its identity and willingness to abide by certain rules. The AC in this study, takes form of an $hq$ delegated privilege that authenticates and authorises or entitles a subsidiary to solicit PzI not exceeding its issuer and provide personalised services for a given time period. The $hq$ by virtue of their enforced policy is authorised to solicit certain PzI and may delegate this privilege to subsidiary $r1$ by issuing $AC^{r1}$ for $meRequest^{r1}$ by signing such that:

$AC^{r1} = S_{hq}\{meRequest^{r1}\}$ The $I$ may alter the delegate validity and authorisation elements of the $S$'s $meRequest$ before the signing. Furthermore, the subsidiary's $meRequest$

differs from the *hq* as it lacks the CA and EA credential elements. Suppose, $delegate = false$ at $r1$ and $delegate = true$ at $r2$, then $r2$ can further delegate its privileges to $l1$ creating a *chain of trust* while $r1$ may not. For $l1$ to solicit PzI from John, it presents its $meRequest^{l1}$ and a chain of ACs starting with its $AC^{l1}$ issued by $r2$, $AC^{r2}$ issued by *hq* that he trusts as Figure 4.1 depicts. Thus, John can verify that $r2$ has delegated his privileges to $l1$ and $r2$ is authorised to solicit PzI by *hq* that controls the service. Subsidiaries then inherit the trustworthiness of the *hq* enforced policy. Therefore, if a customer trusts *hq*, they transitively trust its subsidiaries and can authenticate them.

## 4.2 Service authorisation to PRS

The PRS resides at a user's secure home or work premises and stores portions of their PzI which may be disclosed to authorised requests on behalf of ME2.0. In this respect, the PRS acts as an extended storage for PzI. Alternatives for PzI storage locations and their considerations are detailed in [72]. The starting points for the considerations are storage at the user, the service and third parties. Different locations highlight different challenges such as synchronisation, accuracy, single points of failure, capacity, performance, security and privacy concerns [72]. Nonetheless, motivations for the PRS extended storage and need to disclose PzI on the mobile terminal's behalf are:

- Some PzI change so infrequently that storing them at the PRS may conserve storage on their mobile terminal for more frequently updated information.
- Some resource files, such as detailed *meReply* might be too large to effectively disclose to services over a Bluetooth connection.
- The high cost of accessing Internet services in a foreign country using ME2.0 on the host.
- When in a public area with a suspiciously insecure network, disclosure of PzI might expose ME2.0 to compromises.

The delegation involves the user granting limited authority to the PRS to disclose their PzI to authorised services on their behalf as Figure 4.2 depicts. The articulated security policy permits anyone (i) owning an authorised service and (ii) is in close proximity with the user to get the users preference information from the PRS. The first part of the delegation not depicted in Figure 4.2 is the S/KEY [85] composition [102].

In addition to storing John's password *phrase*, the value $H = F(phrase)$ is stored. A factor that relatively eases authentication considering that $F$ a *hash* function, is trivial to compute from any *phrase*. Computing a sequence of 100 values by successive application of $F$ produces a sequence of 100 passwords [85].

$F^{99}, ..., F(F(F(phrase))), F(F(phrase)), F(phrase), phrase.$

The sequence of $H_i$ required to authenticate these passwords are

$F^{100}, ..., F(F(F(phrase))), F(F(phrase)), F(phrase).$

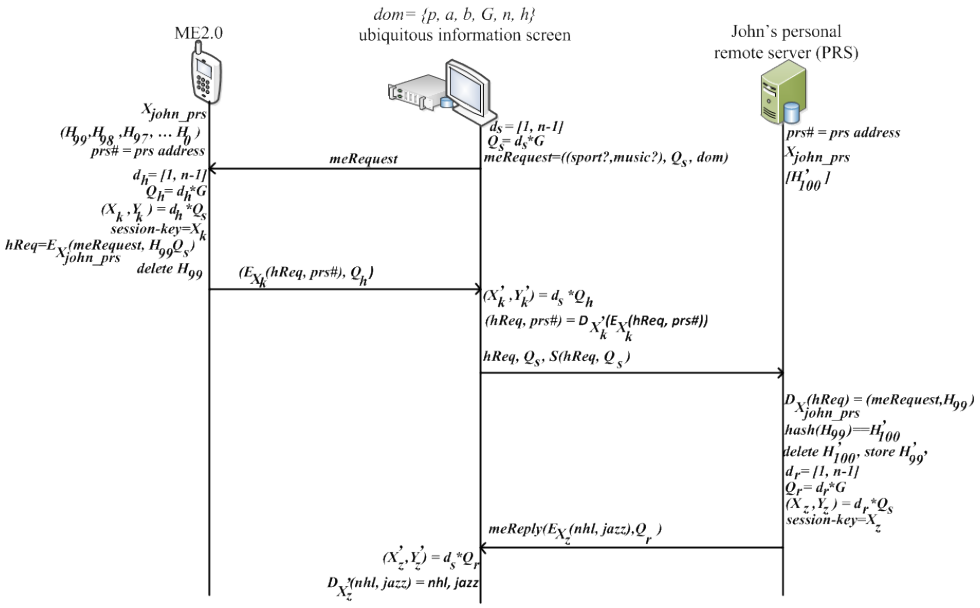



**Figure 4.2:** PRS authentication process.

This recursive $F$ computations result in the S/KEY sets $[H_{99}, H_{98}, H_{97}, ..., H_0]$ and $[H'_{100}, H'_{99}, H'_{98}, ..., H'_1]$ that ME2.0 utilises to grant one-time authentication of the service to PRS. The S/KEY authentication mitigates threats over insecure public networks susceptible to eavesdropping and reply attacks. This approach is similar in principle to that employed by financial institutions [102] in their one-time based codes. The S/KEY is beneficial to mobile terminals due to its portability across terminals, ease of carry, does not demand extra skill to use, no software installation on terminals is needed, and it easily combines with other authentication strategies.

The transfer of S/KEY set $[H_{99}, H_{98}, H_{97}, ..., H_0]$ to ME2.0 is conducted in advance over a secure network at John's home or work. Any subsequent request to ME2.0 for PzI from a ubiquitous service over insecure network is handled as in Figure 4.2. The *meRequest* and the next $H_i$ ($H_{99}$) are encrypted with the symmetric-key $X_{john-prs}$, known only to ME2.0 and PRS to formulate the *hReq*. The *hReq* is then concatenated with the PRS's address (*prs#*) and encrypted again with session-key $X_k$ and transmitted to the service along with its digest for integrity checks and ME2.0's public-key $Q_h$. The $H_{99}$ is deleted from the set in ME2.0.

The service verifies the transmissions integrity before computing the session-key $X'_k$ used to decryption revealing *prs#* and *hReq*. The content of *hReq* is not revealed to the service. The *hReq* is transmitted to the PRS which decrypts it using the symmetric-key $X_{john-prs}$ and then hashes $H_{99}$. If it identical to the current hash at the top of its set, $H'_{100}$ then the request is considered authentic and $H'_{100}$ is deleted. If the hashes are not identical, it is first considered a synchronisation error that PRS attempts to resolve through comparisons with subsequent $H'_i$ until either a match is found or the set exhausted before discarding the request as a malicious. The PRS then computes a session-

key $X_z$ shared with service to encrypt the PzI before transmitting it. The information screen handles the transmission as a standard *meReply* decrypting it to display and play the audio John prefers. On the service attempts to replay old *hReq* they fail as the hashing of $H_{99}$ does not result to $H'_{99}$ and the synchronisation is unsuccessful.

## 4.3 Verifying and validating services

In this thesis, *"privacy"* is an important quality attribute to users. Assuring users of the privacy of their disclosed PzI, implies guarantees on their processing in privacy preserving manners. Services receiving and processing disclosed PzI should undergo rigorous verification and validation. Qualitatively, verification then is a *quality control* mechanism that evaluates the extent to which services comply with imposed privacy expectations. Validation follows as a *quality assurance* process providing evidence that a service accomplishes its intended requirements. The goal of service validation is to confirm that service providers *are building the right service* while, verification seeks to establish *if the service was built right* and correctly implemented. Deeper privacy assurances are attainable using an independent disinterested third parties to verify and validate the service. In the ME2.0 and services interaction, two situations requiring verification and validation are:

1. ME2.0 verifying the authenticity of services they intend to disclose PzI to.
2. Validate that disclosed PzI are handled in accordance to privacy expectation.

The first situation is easily mitigated using mutually trusted CA than the second situation that is often more challenging to mitigate convincingly.

A brief anecdote of the restaurant establishment process sheds some light on how to address the situations simultaneously. In the establishment of a restaurant, the owner has to be verified and validated. First, before the restaurant is established, the owner submits plans to relevant authorities for review and approval. This is basically a validation exercise that paves the way for the owner to submit an application for a health permit. A successful health permit application gives permission for inspection or verification of compliance with the food code by public health specialist. To ensure compliance health inspectors often visit the premises unannounced. Penalties for failure to comply often include heavy fines or even closure of the establishment. The severity of these penalties aims to discourage owners from contemplating taking any risks.

In the absence of a clear and unambiguous means to verify and validate a service, ME2.0 may not guarantee the privacy of PzI disclosures. To ensure privacy assurance for PzI pieces, all services accessed by ME2.0 ought to complete a three step verification and validation process illustrated in Figures 4.3 and 4.4.

In the first step depicted in Figure 4.3, the service composes its credentials which include its public-keys (for encrypting and signing) and identity parameters (ownership, *bdaddr* and so on). The Elliptic Curve Digital Signature Algorithm (ECDSA) [62] is used for all signing purposes. The service signs these credentials and transfers them to the CA mutually trusted by users and services. The CA independently verifies the ownership of the credentials to the named service before signing the credentials ($S_{ca}(credentials)$).

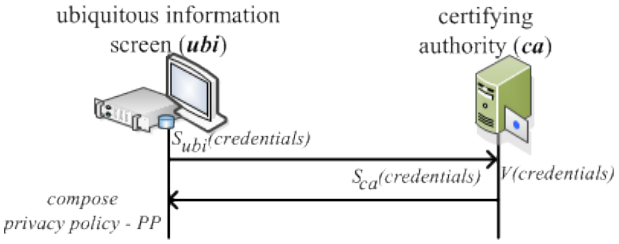



**Figure 4.3:** CA step in service verifying and validating.

The service receiving $S_{ca}(credentials)$ computes its privacy-policy ($PP$) in order to initiate the second step depicted in Figure 4.4. The service selects an EA to enforce its privacy-policy. The service then signs its $PP$ and transfers it to the EA along with its $S_{ca}(credentials)$.

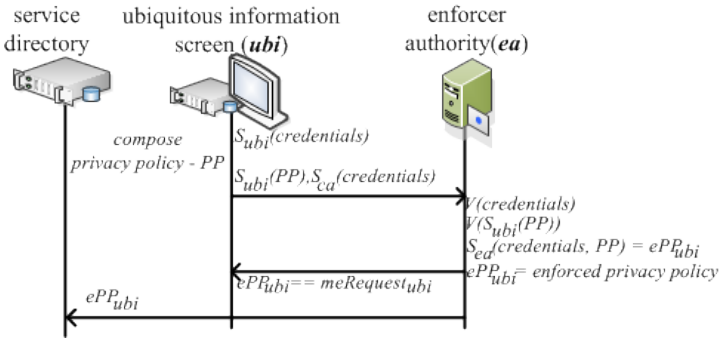



**Figure 4.4:** EA step in service verifying and validating.

At the EA both the $PP$ and $S_{ca}(credentials)$ are verified again before being bound together by the EA's in $S_{ea}(credentials, PP)$. This policy document ($S_{ea}(credentials, PP)$ or $ePP_{ubi}$ or $meRequest^{ubi}$) is then enforced and the credentials owner is considered verified. To effectively serve in this capacity, the EA is provided with sufficient authority to penalise non-compliance. The EA penalties are severe enough to discourage non-compliant services, in a manner similar to the restaurant establishment scenarios. This important EA role is best performed by an independent industry or government appointed institution. The role of EA include:

- Verifying credentials in privacy-policy independently of the CA and services.
- Eliminating overlaps where a service attempts to enforce multiple privacy policies to solicit different intersecting PzI.
- Binding the service credentials to their privacy-policy thereby validating the service.
- Publishing enforced policies to the service directory allowing all stakeholders to view, query, select and enlist the service.

- Invalidating enforced policies due to non-compliance with services request or other reasons. All decisions on services privacy policies are published at service directories.
- Inspecting PzI handling by service unannounced without warning or due to user complaints.
- Penalising non-compliant services that inappropriately handle users PzI. Worth noting is that EA is not concerned with what types of PzI services solicit from user rather on there handling as indicated in their privacy policy.

In the third step ME2.0 obtains the enforced policy $ePP_{ubi}$) from the service directory or the service on the fly. This is an independently verified and validated request document presentable to in soliciting PzI. With the $ePP_{ubi}$), ME2.0 users can filter, select and enlist enforced policies matching or exceeding their privacy expectations from the service directory. Users' privacy expectations are composed from their disclosure policy documents. These documents detail the PzI they wish to disclose and their handling expectations. On enlisting services meeting or exceeding their privacy expectations, users are assured of verified and validated enforced policy with channels for redress in case of suspected misconduct. The actual PzI users' disclose are those intersecting on their handling such that: $meRequest = \{sport?, film?, music?\}$

$dp_john = \{age?, sport?, music?\}$

$dp_john \bigcap meRequest = \{sport?, music?\}$

$meReply_john = select(dp_john \bigcap meRequest, PzI)$

$meReply_john = \{NHL, Jazz\}$

This mutually shared $ePP_{ubi}$ or $meRequest^{ubi}$ by services and ME2.0 is also important in enabling the exchange of cryptographic information to authenticate the entities and ensure confidentiality of disclosed PzI.

## 4.4 Discussion

The discussions about the feasibility of ME2.0 in disclosing users' PzI to different services with different configurations has been demonstrated. Also considered alongside these demonstrations is the preservation of users' PzI privacy when desired and in untrustworthy environments are presented. Combing this feasibility and the privacy preservation possibilities opens new avenues for more exciting solutions. Context-awareness has a significant part in the form of S/CI where appropriate content is displayed at appropriate times as well as limiting the amount of PzI disclosed. More sophisticated use cases of ME2.0 are possible for the assistance for elderly citizens.

More study is needed to streamline the use of AC with the stated SPKI, with more emphasis placed on their performance, privacy and their delegation. In particular, details on formalising and understanding delegation with certificates in networks in terms of their construction, deletion and reductions are needed. This warrants further evaluations of ME2.0 from perspectives discussed in [11].

Further analysis is needed to determine the extent of privacy and security compromises when the same keys are used for both signing and encryption. In particular the evaluation on the interaction of the keys when used in ECDH and ECDSA computations is needed.

Chapter V

# Usability of ME2.0

So far, the discussion of ME2.0 has covered its architecture (Chapter 3) and the different manners of its use (Chapter 4). In this chapter, the usability of ME2.0 will be evaluated in comparison with alternative solutions. To accomplish this, it is important to identify stakeholders attached to different features of the application. The usability evaluation should then focus on those features identified as of the highest priority to key users.

There are numerous features in ME2.0 that can be evaluated from different stakeholder perspectives. Rather than considering all features from all perspectives this chapter prioritises usability, performance and privacy preservation from the users' perspective.

## 5.1 Usability criterion

Seven features define the similarities between ME2.0 and other user applications include: having a functional Graphical User Interface (GUI), the need for user input, giving user feedbacks, user feeling of being in control, user consent, and notifications to users. Based on these similarities, the importance users generally place on other different features of the applications can provide guiding indicators of where ME2.0 should focus its attention on to improve its usefulness and appeal.

The study considered here was conducted at Lappeenranta University of Technology, in which 1365 students of different genders, age groups, nationalities and computer competencies participated [70]. The aim of this study was to identify and rank the features of the application in a hierarchical order of importance by the target group. The study considered the priorities of the 21 different features that included: *accessibility, aesthetics, brand, consistency (of functionalities), coolness (wow effect), device (where the software is used), emotions, used environment, expectations, functionality, interaction, motivation, pleasure, purchase price, reliability, stability, trust and privacy, usability, usefulness, user interface* and *ease of taking into use.* The importance attached to each feature was ranked on a Likert-type scale (1 - very important, 2 - important, 3 - moderate important, 4 - of little importance, 5 - unimportant, and 6 - don't know/understand).

The data from the users were subjected to statistical analysis of variances that included computations of the mean, variance, standard deviation and mean deviation as shown in Table 5.1.

**Table 5.1:** Importance attached to features and functions of software

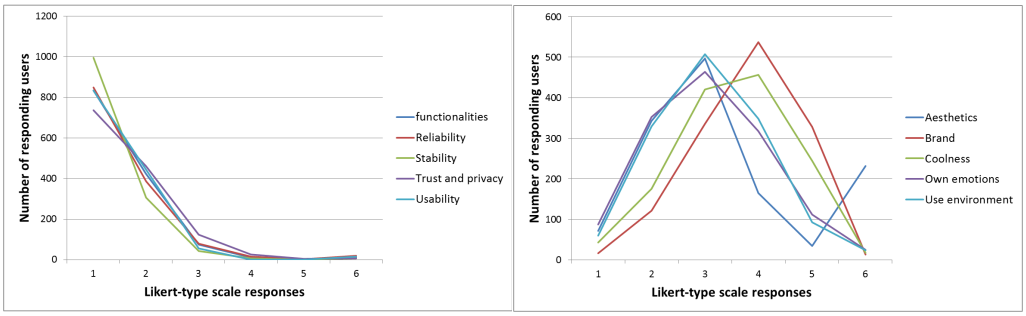
| Features | Mean | Variance | Standard DEV | Mean DEV |
|---|---|---|---|---|
| accessibility | 1.92 | 1.18 | 1.09 | 0.70 |
| aesthetics | 3.33 | 2.14 | 1.46 | 1.17 |
| brand | 3.80 | 0.96 | 0.98 | 0.79 |
| consistency | 2.14 | 1.79 | 1.34 | 0.90 |
| coolness | 3.54 | 1.14 | 1.07 | 0.90 |
| device | 2.76 | 1.28 | 1.13 | 0.90 |
| own emotions | 3.07 | 1.25 | 1.12 | 0.87 |
| use environment | 3.12 | 1.10 | 1.05 | 0.81 |
| own expectations | 2.73 | 0.96 | 0.98 | 0.78 |
| functionalities | 1.49 (3) | 0.60 | 0.77 (2) | 0.61 |
| interaction | 2.41 | 1.26 | 1.12 | 0.88 |
| own motivation | 2.50 | 1.08 | 1.04 | 0.84 |
| pleasure | 2.67 | 1.12 | 1.06 | 0.85 |
| price of purchase | 2.36 | 1.40 | 1.18 | 0.96 |
| reliability | 1.53 (4) | 0.78 | 0.88 (5) | 0.66 |
| stability | 1.34 (1) | 0.44 | 0.66 (1) | 0.49 |
| **trust and privacy** | 1.62 (5) | 0.68 | 0.83 (4) | 0.67 |
| **usability** | 1.48 (2) | 0.60 | 0.77 (3) | 0.60 |
| usefulness | 1.91 | 1.12 | 1.06 | 0.76 |
| user interface (UI) | 2.40 | 1.86 | 1.36 | 1.01 |
| ease of taking into use | 2.05 | 0.95 | 0.96 | 0.71 |

A smaller mean value or weighted mean (Appendix II) implies that users attached higher importance to the particular feature. From Table 5.1 it is noted that with the exception of stability and reliability, the short-listed features of ME2.0 rank within the top five important features for the users.

Mean values do not provide much information on the diversity of the features ranked by the users. Table 5.1, calculates the standard deviation because it reveals the dispersion from the normal among the population. Statistically, a lower standard deviation value implies a majority of the data points were closely clustered together around the mean while a higher value implying they were widely spread out over a large value range. Figure 5.1 derived from Appendix II confirms that users placement and ranking of most important features (Figure 5.1a) was common for more users compared to those of Figure 5.1b.

## 5.2 Usability study

The results from the study in Table 5.1, suggest that focusing on the usability of ME2.0 is likely to be appreciated by the users. However, ME2.0's usability is of slightly different

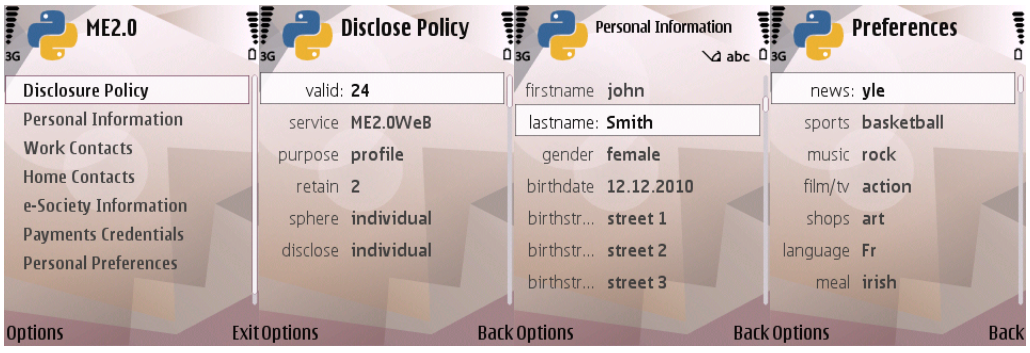



(a) (b)

**Figure 5.1:** Most important and least important features to users.

nature. ME2.0 is an application of the ubicomp domain. Ubicomp applications are often viewed as *"the next age of calm technology, when the technology recedes into the background of our lives"* [150]. It has often been asserted that ubicomp applications should mimic an invisible servant who performs more duties by intuition and creates calm [150]. Brown [26] articulates a calm technology as that which *"informs but does not demand our focus or attention"*. Given this, the findings of the study above suggesting that users prefer a clear and easy to user UI to be an important goal for ME2.0 usability.

The starting point ME2.0 UI depicted in Figure 5.2 was implemented on a Nokia N95 mobile terminal. On starting ME2.0 the user is presented with a view of Figure 5.2a screen that presents various categories for configuring ME2.0. The selection of an intended service to disclose PzI and its handling expectations that directly affect users' disclosure policies are configured in Figure 5.2b. Users' configure their PI and P/GPref in UI screens illustrated by Figures 5.2c and 5.2d respectively.




(a) (b) (c) (d)

**Figure 5.2:** Initial UI for ME2.0.

To improve the ME2.0 UI depicted in Figure 5.2, usability aspects are based on key user needs gathered from interviews, surveys, prototypes and field evaluations. In addition,

preferred UI design layout, privacy manageability and consensus UI design comprehension are evaluated. Clarity of priorities in ME2.0 is shaped by usability studies to effectively increase target user acceptance.

Four studies were conducted to improve the UI by extrapolating and evaluating a suitable UI for ME2.0. To minimise leading the of participants, ME2.0 is referred as *software-XYZ* in the study scenarios. The studies conducted were: initial usability interviews, UI design prototypes, Internet-based survey and Wire-frame prototyping.

### 5.2.1 Initial usability interviews

The initial usability study recruited 9 participants (Table 5.2) to evaluate their attitudes towards needs and preferences for personalised services. Scenario evaluations were presented in group interviews to broadly elicit attitudes towards personalised mobile services and provide some background on the research domain.

The respondents for the study comprise four females and five males. Seven of these respondents were aged between 18 and 30, while one was in the 31 - 49 age-bracket and another one in 51 - 60 age-bracket. No respondent was found in the 41 -50 age-bracket. In terms of professional inclination, three respondents were students and the remaining five were respectively a researcher, an engineer, a salesperson, a financial specialist, an IT support technician, and a utility/electricity technician. Furthermore, the respondents had differing levels of computer proficiency. In terms of their computer proficiency, three were considered to be at the basic level, and another three at intermediate level. Of the remaining three,two were considered to be experts and one proficient.

In terms of mobile phone usage, five indicated that they have one phone, while the remaining four had two to three mobile phones. Of these phones, four were smart phones. In terms of Internet accessing phone software, two respondents indicated that they use Spotify and five use E-mail. Radio, Facebook and maps users were respectively two, three and one.

Table 5.2 contains the responses obtained from these respondents on whether or not they liked software-XYZ.

Future possibilities for personalised services were then presented to the participants as a scenario in everyday life. In this study, 9 respondents of varying demographics and backgrounds participated. The selection process sought to achieve some balance amongst participants in terms of gender, age and computer skills. The participants were then divided into two groups. Most participants were aged between 18 - 30 years, with a few aged 51 - 60 years. The participants had different levels of experience with personalised Internet sites like Amazon and eBay. Three scenarios (*scenario-1, Scenario-2, Scenario-3*) were developed to guide focused discussions on different aspects of personalised services. *Scenario-1* sought to evaluate participants attitude to installing an application in their mobile terminals that is then used to personalise ubiquitous services by disclosing pieces of their PI.

***Scenario-1**: You have installed software-XYZ on you mobile phone. This new software uses your Personal Information contained in your mobile phone such as age, language, gender, preferred restaurant, credit card numbers, bank account number, passport number,*

**Table 5.2:** Participants opinions on software-XYZ

| **Feature(s)** | Participants opinions |
|---|---|
| Liked features | Opens opportunities(1)<br>Eases life(2)<br>Finds my interests/preferences(1)<br>Service personalisation(3)<br>Simple and straight forward(1)<br>Pay bills with it(1) |
| Disliked features | Gives out my PI(2)<br>Others know my interests(1)<br>Too many passwords(1)<br>Complicated(1))<br>Security, privacy and trust(1)<br>Knows too much about me(1) |
| Suggested features | Security/privacy/trust(4)<br>Ease of use(1)<br>Personalise shopping experience(1)<br>Different levels to give PI(1)<br>Locate interesting events nearby(1)<br>Locate favourite shops(1)<br>Locate child friendly places(1)<br>Remove private data(1) |

*sports preference, hobbies, music genre and meal preferences to personalise services in your surrounding environment and display preferred information.*

*Scenario-2* progressed closer to the actual usage of ME2.0 with the intention of giving participants a real life situation where personalisation would be useful without emphasising the usage of PI directly.

***Scenario-2:*** *One week later you travel to Tokyo, Japan. As you do not speak or understand Japanese, software-XYZ installed in your mobile phone automatically informs the airport information screens about this and immediately all the information is also translated from Japanese to the native language set in your phone. This occurs with all information screens and notice boards you come into close proximity with at the airport.*

*Scenario-3* advances *Scenario-2* by adding more PI to bring privacy into perspective. The depicted service explicitly requests PI with financial implication. The purpose of *Scenario-3* is to evaluate changes in participant responses by disclosing more PI that is sensitive in nature.

***Scenario-3:*** *Thirty minutes later, you are walking by a small mall in down town Tokyo looking for a decent restaurant. Digital billboards close by are continuously translated into your native language. The content displayed on these billboards changes to your preferences. The result is you receive directions to the closest restaurant matching your meal preferences on your mobile phone. In the restaurant the music automatically changes*

*when you enter and you receive the menu filtered by what you can eat. The waiter comes to your table you place the order and later pay automatically with your phone.*

The participants all responded to the initial interview questions. The questions generated discussions on the control of software-XYZ, mechanisms to protect PI, decisions on service selection, grouping of PI, additional preferred features, functionalities that should be withdrawn and preferred notification manners. The initial 8 open ended questions were:

- Question-1: How much control would you like to have on software-XYZ?
- Question-2: How would you like to protect your information in software-XYZ?
- Question-3: Where and when would you like this protection?
- Question-4: How would you decide on what services to trust and not to trust?
- Question-5: How would you group your PI?
- Question-6: What else would you like in software-XYZ that is currently not there?
- Question-7: What would you like to remove from software-XYZ that is currently here?
- Question-8: What kind of notifications would you like from software-XYZ?

The open ended questions were then focused after consultations with a usability expert to target very specific responses and presented to a wider community of participants using Internet survey tool Webropol [149].

#### Interviews findings

On *Scenario-1*, all participants had sufficient overall comprehension of the scenario without additional explanations or alternative scenarios. On the usefulness of software-XYZ in *Scenario-1*, four of the participants strongly agreed, three participants and the remaining two participants remained non-committal to either side. Privacy concerns regarding PI in the scenarios generated discussions among the participants. Participants conveyed concerns for their *"critical information"*, as one respondent termed credit card, bank account and passport number. Additionally, 5 of the participants had privacy reservations with their age and preferences. Of the participants concerned about their age and preferences, the majority (6 participants) had more concerns about their preferences than age.

All participants straightforwardly and quickly responded to *Scenario-2*. Some participants offered further uses of software-XYZ such as, *"it would be nice if my phone informed me of the best mode of transport, the cheapest or the most attractive"*. *Scenario-2* raised positive attitudes among the participants except for one single participant who questioned his intentions on learning the foreign language. No privacy concerns arose with *Scenario-2*. Two participants engaged in a discussion on the best way to notify the screens about the language they preferred considering they were multi-lingual.

Intentionally, *Scenario-3* positioned participants beyond the relatively secure airport environment by using software-XYZ context-awareness in the wild. The scenario's comprehension by all participants was above average as they related it with previous scenarios and group discussions. Despite participants' attitudes remaining high on the usefulness, the mention of all billboards translated to the participants' native language raised questions on control, notification and consent. Just over half of the participants (5 participants) remained unconcerned about personalising the billboards. Of the remaining four participants one wanted total control of which billboards were translated, while the rest (3 participants) desired marginal control through *"pre-sets", "ignore previously seen,"* or *"download billboard content to terminal"*. The navigation service in *Scenario-3* to the nearest matching restaurant was considered useful by all participants. However, disagreements emerged on personalising the restaurant's environment and mobile payment. Five of the participants were fully content with the restaurant personalisation to their preferences such as music and news. Three participants wanted no influence on the restaurant environment and suggested that they prefer to leave things as they are in respect of natural settings, staying anonymous, and not imposing their preferences on others.

On the mobile payment scenario, three of the participants were willing to accept mobile payment, two participants wanted absolutely no payment conducted with their mobile terminal for security reasons, inquiring what if the mobile terminal was stolen or misplaced. The remaining participants (4 individuals) preferred the option of deciding to accept or decline the means of payment such as cash, credit card or mobile behind a secret number.

Participants had subjective responses to the 8 open ended questions in Section 5.2.1. The questions were first posed to individual participants and then later to the group for discussion. The responses varied across the participants.

Question-1: Most of the participants had strong views regarding control of software-XYZ, with 4 of the participants desiring total control and three wanting to be mostly in control. The remaining participants were undecided either way.

Question-2: All participants preferred some stringent protection for their *"critical data"* like credit cards, passport and bank account numbers. PIN codes were preferred over passwords by two of the participants. Surprisingly, the protection for PzI that had no ties to financial obligations was considered unnecessary.

Question-3, 4 and 5: Five of the participants suggested a form of TTP role by either the police, government, banks or mobile applications on-line stores to provide the list of acceptable services alongside their trustworthiness and reputation. One participant took the pragmatic approach of distrusting all services until they had being sufficiently tested. The remaining participants suggested they would only base their decision on recommendations from experts, friends or colleagues. The participants categorised their PI into various forms. The prevalent categorisations were critical (credit card, passport and bank account number) and non-critical (language, age) this information was given by 7 of the participants. The remaining participants added extra categories such as any information identifying me and payment information.

Questions 6, 7 and 8: Focused on software-XYZ improvements from the participants' perspective. Discussions among participants about these questions raised a general aware-

ness of privacy hazards and related technologies that presently compromise their privacy. Nonetheless, the participants pointed out the following additional features to be desirable:

- Ease of use and convenience UI (2 participants)
- More security with different levels or modes (6 participants)
- Adjustable notifications/information (5 participants).

One participant emphasised the need to remove all PII from software-XYZ, while another emphasised the need for software-XYZ to be efficient and fast. The replacement of passwords with PIN was raised once again.

On the features to be excluded from software-XYZ, six participants' agreed on identifiable information, two of the participants on excessive notifications and one participant agreed on passwords and traceable data. While discussing notification appropriateness in Question-8, one third of participants preferred the notices to be similar to Short Message Service (SMS) but distinguishable from existing settings of received SMS, E-mails or alarms. Two participants insisted on having all alerts (ring, vibrate, flash) when PI or payment credentials were about to be disclosed. The remaining participants were divided between different notifications at different times of the day and situations. One participant was keen on having no notifications just a log for later review on which disclosures to which services had been made.

### 5.2.2 UI design prototype

After the scenario discussions and interviews in Section 5.2.1, each of the participants was given a blank mobile terminal idea-sheet illustrated in Figure 5.3 and asked to design a suitable prototype UI layout and navigation for software-XYZ they prefer to use. During the prototype design participants verbally expressed their design intentions. The participants were also questioned to gain better insight into their motives for the different designs and how to navigate the UI.

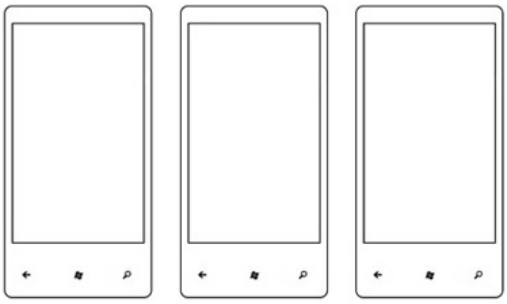


**Figure 5.3:** Participants idea-sheet for designing a suitable ME2.0 UI

### UI design findings

Six of the participants sketched reasonable UI designs prototypes expressing some clear organisation of icons, screens, screen layouts, and navigation. The remaining three participants were only able to discuss and express their UI ideas verbally or using their mobile terminals as reference points. The most notable UI design prototypes suggestion from the participants was the need for a simple but complete landing screen. Participants preferred the landing screen to depict all elements in simple groups without the need to scroll up or down to see the entire list. Additionally, the use of related icons along the element names was expressed. The dominant landing screen layouts by participants are depicted in Figure 5.4.

In addition to the simple and straight forward landing screens in Figure 5.4, the participants expressed the need for visual aids displaying currently available services and disclosed PI without fidgeting with their mobile terminals. Unfortunately, none of the participants could articulate the mentioned visual aids in a design until one participant suggested a ticker like widget that continuously scrolled at the top or bottom of all screen to display all vital information. To this ticker participants would add or remove any information they wished to monitor constantly. A colour coded icon or text depicting the current state of software-XYZ was also considered as an alternative to the ticker.

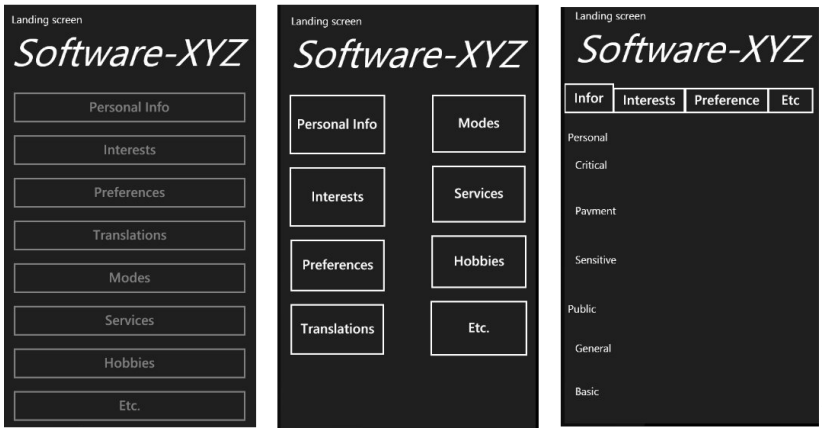



**Figure 5.4:** Common UI landing screens layouts by interviewees.

Five of the participants expressed the need to group and disclose different groups or sets of PzI under *modes, profiles* and *settings*. Of the five participants, three used the term modes, with one participant commenting *"it would be nice to have different modes like free-time, business and bar mode with different PzI or versions of PzI"*. Another participant added that they *"would also like to add shopping and mother-with-infant mode"*. The remaining two participants used the terms profile and settings to distinguish groups of PzI. Suggested profiles and settings included *store-profile, me-profile, citizen-profile, staff-settings* and *student-settings*. Based on the participants' UI prototype designs and discussions with usability and security experts, a consolidation of the UI elements in the landing screen depicted in Figure 5.5 was developed. The landing screen is termed consensus UI.

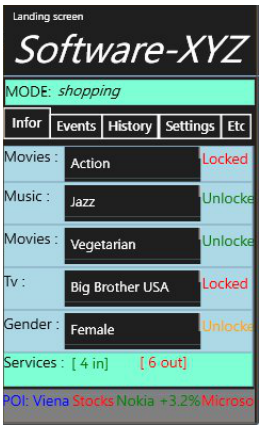



**Figure 5.5:** Consensus UI

The consensus UI was then presented to four of the initial participants for comments, alterations and evaluations.

### 5.2.3 Internet-based surveys

Refinements to the initial usability interviews in Section 5.2.1 eliminated questions considered unnecessary to investigate further the usability of software-XYZ. For instance, the inability of participants to compose meaningful use scenarios for using software-XYZ resulted in a refinement of the description as mobile phone software. Some questions were also merged or co-joined and new questions were formulated, while others were re-structured or re-grouped to emphasise important aspects. The objective was to conduct progressively refined Internet surveys iteratively to saturation when no new further information was forthcoming. Towards this goal, three Internet survey iterations were realised with four participants in each group. Figures III.1, III.2, III.3 and III.4 in Appendix III depict the final survey iteration.

*Iteration-1* was composed of 26 open ended and eight Likert scaled questions covering various aspects of software-XYZ. The questions targeted the following aspects of personalised services in mobile terminals:

- PzI in the terminal
- The classification and organisation of PI pieces
- Levels of control or automation
- Notifications or feedback
- Privacy
- Security and trust

The open ended questions elicited personalisation relevant information that would affect the usability of software-XYZ. The open ended questions were structured to relate them to familiar terms and concepts like GPS and calendars as sources of PzI. The Likert-type questions provided four ranks of opinions from strongly-disagree, disagree, agree and strongly-agree. The responses from *Iteration-1* were discussed with usability experts and compared with the results of the initial study. The outcomes of these discussions were refined for used in *Iteration-2*.

The second iteration was shorter with 16 open ended and eight Likert scaled questions. The survey questions had been further refined and reorganised in the questionnaire layout. Related questions were placed next to each other in the same page view and similar concept questions were combined. An entirely different set of four participants was enlisted for the *Iteration-2* survey. The refinements generated more accurate responses from participants. The majority of the participants' responses were similar to *Iteration-1*, with a few exceptions offering new information and views on usability previously unconsidered. The presence of new views prompted a further refinement.

The third Internet survey iteration *Iteration-3* was the final survey iteration because it did not generated any new usability dimension nor previously unseen participants responses. Similar to previous iterations, four respondents participated in the final survey.

#### Internet-based survey findings

Demographically the Internet-based survey was more diverse compared to the initial usability testing in Section 5.2.1. Participants displayed more diversity in their backgrounds, ages and computer skills. Thirty percent of the participants were aged 26-30 years, 40 percent 31-35 years and the remaining 30 percent were above 36 years but below 67 years of age. Female participants comprised 60 percent of the participants recruited for the survey. Participants had diverse career backgrounds like sales women, system administrators, environmental engineers and IT students and were spread across nine cities and eight countries.

The three iterations were conducted deductively with a sample population of four participants each until no new additional information was generated. *Iteration-1* participants provided 21 unique types of PzI to store on their mobile terminals. *Iteration-2* participants had 14 additions to *Iteration-1*'s list of PzI. The third iteration provided only synonyms and examples of PzI already provided by previous iterations.

On classifying the PI, all iteration participants had mostly similar groups such as payment, personal, contacts, interest/preferred, secret and events/reminder/calendars. A respondent from *Iteration-2* added icons and keywords for further classifications.

On allowing software-XYZ to transparently or automatically solicit users listed PI and preferences, distinct patterns were noted across all iterations in permitting solicitation of generic, non-identifiable and impersonal information pieces like contacts, and messages. On the contrary, payment credentials, critical and identifiable information were excluded in the automatic solicitation list.

*Iteration-2* participants provided more concise details compared to both *Iteration-1* and *Iteration-3* participants. *Iteration-3* participants were more focused on appropriate manners of using software-XYZ to disclose information from them. *Iteration-1* list consisted

of phrases like *"so and so has shared new contact information, would you like to update their contact details rather than your contacts have been up-dated"*. In contrast the list from *Iteration-2* participants included pop-ups, vibration and on-screen icon. The question on the retention duration of solicited PzI was uniformly attended to across all iterations with durations like daily, weekly, whenever there is new information and per session for payment credentials.

Aggregating the participants' opinions on how they preferred software-XYZ to identify them, 54.5 percent opted for passwords, 27.3 percent for a secret number or PIN code and 18.2 percent for biometric identification like fingerprints and voice recognition.

The service selection question indicated that majority of participants would rather be informed of available services at their disposal, than manually searching for them. One participant expressed the desire for a service registry where they could select a service by typing. Another participant was keen for both service recommendations and manual selections. Inquiry about trusting a service proved ambiguous with *Iteration-1* participants and was therefore dropped from subsequent iterations. On preferred anonymity levels for software-XYZ, all iteration responses were vague. Only four alternative anonymity modes were suggested: as anonymous as possible, anonymous for some uses like payments, default anonymity and modifiable anonymity.

Activities with cost implications received the most attention from interviewees when discussing about instances of activities or events they would like to be notified about. *Iteration-1* participants were articulate in expressing that they would prefer to be notified in the event of cost, security and privacy implications, new or interesting occurrence or expiration of some service.

On additional desirable features for software-XYZ, most realistic results were noted with *Iteration-1* participants who mentioned security features and ticketing services. However, *Iteration-2* and *Iteration-3* interviewees only repeated examples provided with the question hints. Additional improvements for software-XYZ were security or privacy, responsiveness, clear explanation without IT jargon and ease of use UI. The Likert scale questions results were clearly uniform among the three iterations. 80 percent of the participants were in agreement with the use of context to adapt the logic of mobile terminal. All participants were keen on the UI showing only relevant S/CI.

### 5.2.4 Wire-frame prototyping

Paper prototypes are widely used assets in User-Centric Design (UCD) processes to test UIs for websites, desktops and mobile terminals software. In paper prototyping a single participant is given a screen sketched on a paper with widgets allowing them to explore the overall software scrolls, combo-boxes, buttons and navigations. Wire-frames are paper prototypes in digital formats and extend the benefits of paper prototypes by enabling simultaneous testing with multiple participants who might be remotely located in cost efficient, collaborative and flexible manners. Feedback from participants are either typed or recorded and played back later.

In evaluating ME2.0 with a wire-frame the reference to it as software-XYZ was retained and the SketchFlow [99] was adopted to implement a functional wire-frame, navigation flows, screen layouts and interactive UI elements. SketchFlow adoption was based on its

easy availability at the Laboratory of Communications Software and its ease in depicting advanced application navigations. After implementing the SketchFlow wire-frame, it was deployed on the Internet and participants enlisted and provided the web address to explore the UI and the accompanying screen-map. The UI screen-map is depicted in Figure 5.6 gives the logic of navigating the software-XYZ's wire-frame.

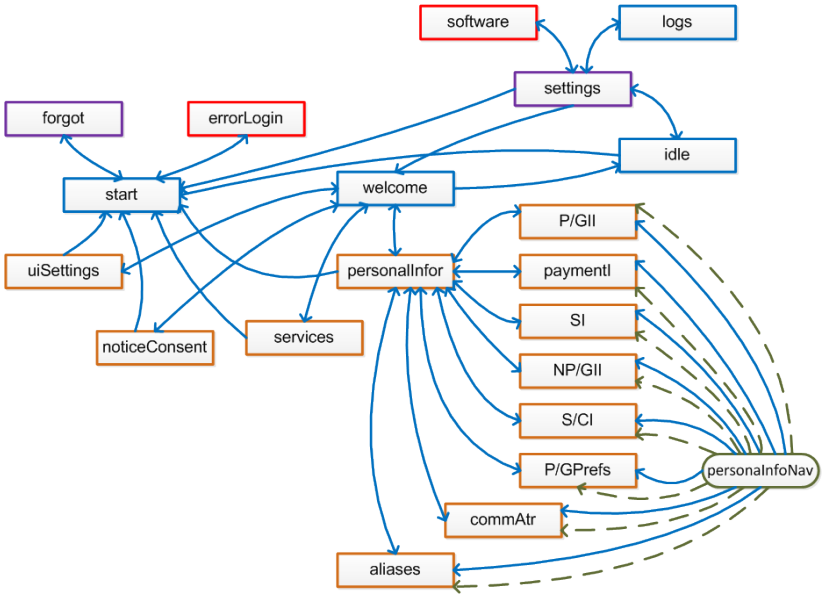
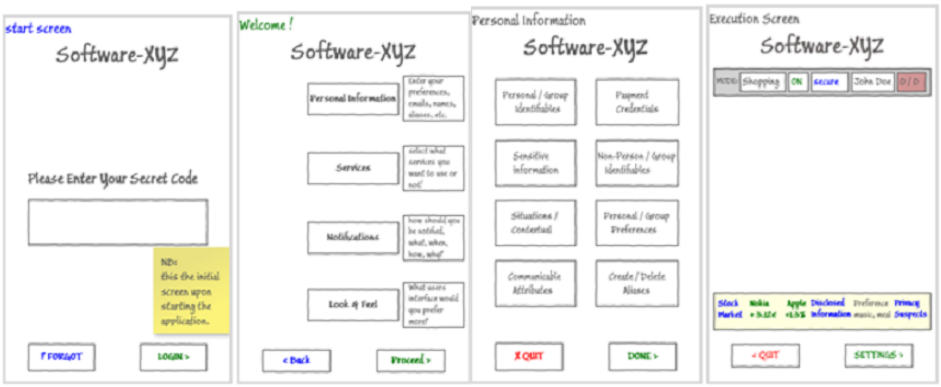



**Figure 5.6:** Software-XYZ UI screen navigation map

The blue boxes are software-XYZ screens in the event no errors are encountered, with the start box as the initial screen. Blue arrows show available navigation paths, for example, one can directly navigate to the idle screen from the welcome screen, but not the reverse. In event of an error the user is directed to the red boxes. The purple box, forgot screen is a convenience screen providing users a means to recover their secret code to change their credentials. The orange boxes are software-XYZ personalisation settings. The main settings relate to UI *uiSettings screen*, notifications *noticeConsent screen*, services and PI *personalInfo screen* settings. Green ellipse *personalInfoNav* is a shared UI navigation component between the eight PI settings.

Software-XYZ screens visible to users are created using the SketchFlow styling that gives a sketchy appearance. The sketchy appearance minimises chances of misleading participants into thinking that it is a finalised version of the software. Nevertheless, the resulting UIs are fully functional artefact enabling users to navigate through the potential software. Figure 5.7 illustrates the start screen (Figure 5.7a), welcome screen (Figure 5.7b), PI screen (Figure 5.7c), and the idle screen (Figure 5.7d). SketchFlow also aids the UI designers to place hints like in Figure 5.7a, for the participants in adding more explanations.

To test the software-XYZ wire-frame, four more new participants were recruited and given the deployment web address and asked to navigate the SketchFlow player depicted




(a) (b) (c) (d)

**Figure 5.7:** UI navigation screens for software-XYZ

in Figure 5.8. The navigation of software-XYZ in the player permitted the participants to obtain an experience of how the final product is likely to feel and behave.

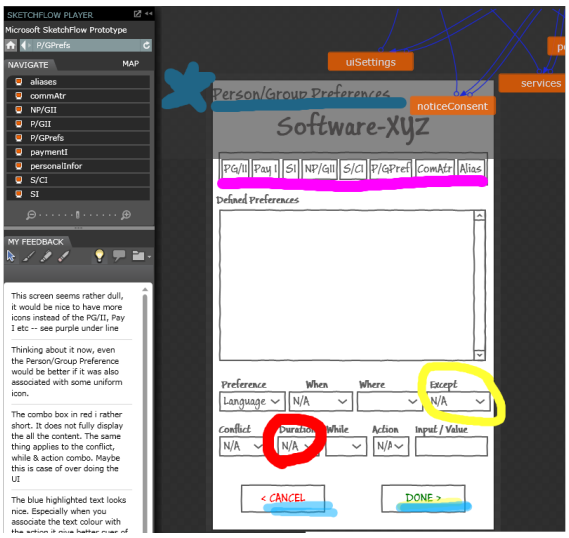



**Figure 5.8:** Software-XYZ SketchFlow player view

The SketchFlow player also allowed users to comment on aspects of the UI wire-frame and highlight any details in expressing their views. Figure 5.8 illustrates some feedback notes and highlights. Once completed, developers could replay the navigation of the software along with the comments and highlights while noting the navigation paths used by the participants.This provides developers with insight into how intuitive the UI was to the users, where the users encountered difficulties and which parts needed improvements.

### Wire-frame findings

The wire-frame prototyping provided two important feedback channels. Firstly, the ability to playback the recordings and visualise how participants navigated the wire-frame UI. Secondly, the participants' comments and highlights on specific aspects of the UI as they navigated.

The wire-frame prototype offered a more practical aspect of the usability study. On the playback results, it was noted that most (82 percent) of the participants navigated directly to the PI (personalInfo screen) and spent the majority (69 percent) of their time there considering what PI were referred to there. The rest of the participants showed clear exploration tendencies in the wire-frame to acquire a feel of what was where and how to get there. A reasonably high number of retracted navigations indicated some error during their navigation. The errors were mostly noticed with the navigation bar on the PI setting screens.

Comments from the participants were mostly on the PI settings screen. The general feel was that the PI screen was too busy and, according to some participants, asked for more detailed information than was necessary. Two participants were concerned about the absence of icons, especially on the navigation bar. Another participant commented on the large amount of information that must be captured manually and that repetition of information on another screen or terminal would be too cumbersome. This same participant suggested an on-line backup on their Personal Computer (PC) that could synchronise the information when using the Internet or a Universal Serial Bus (USB) cable. Other comments included dull screen and non-uniform screens. The idle screen was also criticised for lack of a recycle bin where elements from the ticker could be removed by drag and drop motion. Questions also lingered on whether it was possible to add more tickers on this screen.

The most highlighted aspects of the UI were the combo-box and the navigation bar in the P/GPref screen. The *N/A* item in various combo-boxes was also heavily criticised and highlighted by users citing *"I do not understand this, what does this mean?* And *can it not be more specific?"* The lack of icons on the buttons and the screen title also raised considerable criticism.

## 5.3 Performance

The performance evaluation of ME2.0 considers the overhead in utilising services with security and the increase in communication overhead. From the onset, it is common knowledge that security and privacy mechanisms are traded-off against computation performance. This section seeks to quantify the extent of this trade-off.

The incorporation of security and privacy mechanisms are noticeable in the size and number of messages exchanged between entities and the delay in the entities communications. Sizes and number of exchanged messages directly affect the payload overhead while the delays are depicted as communication overhead. Additionally, it is relevant to consider which specific aspect of ME2.0 security and privacy mitigation strategies are responsibly for which delays.

Fundamental interactions important to consider in the payload overhead are the service and ME2.0. Interactions involving the service and the CA or the service and EA are irrelevant at service access. In effect the size of *meRequest* and *meReply* are ideally affected by the amount of PzI the service defines and the amounts users willingly discloses. Therefore, these values differ across users and ubiquitous services.

In addition to the size and number of communicated messages, the duration of time from when *meRequest* is dispatched to when *meReply* is received are also affected by the security and privacy strategies. There are likely to be greater communication delays when ME2.0 has to verify the authenticity of a service compared to when it is not necessarily to have the authenticity verified. This is even more so when the authentication involves the service directory.

The PRS evaluations involve comparisons of time intervals between dispatching the *meRequest* and actual receiving of the *meReply* as a CnP on the ubiquitous screen. Time values are compared between direct access and direct-indirect service access. Scalability aspects are also taken into account using single and multiple mobile terminals. The size of communicated data is catered for in the evaluations by keeping the amount of requested information and the users disclosure policies identical. The average time taken in seconds for the ubiquitous information screen to dispatch a *meRequest* and receive the corresponding *meReply* from ME2.0 was 0.65594, with a standard deviation of 0.0037. The *meRequest* in the experiment was 661 bytes while the *meReply* was 203 bytes. The ubiquitous screen then decrypts the response and forwards it to the PRS. The PRS's responds with a CnP *meReply* of 268 bytes. The average times and standard deviations for the information screen receive the *meReply* from the PRS is 0.6079 with standard deviation of 0.0170. The overall interaction of the PRS scenario takes an average of 2.2341 seconds with a standard deviation of 0.4723.

The overall time taken using ME2.0 in a direct-access rather than the direct-indirect access of the ubiquitous information screen averaged at 1.5596 seconds with computed standard deviation of 0.1151. The computed measurements depict the interaction from request to final determination of CnPs. The size of *meReply* responses in this instance are 173 bytes.

## 5.4 Security and privacy

Section 5.2 focuses on the visible part of ME2.0, the UI and usability. This section delves into the invisible area behind the scenes.

### 5.4.1 Direct PI leaks

Fundamental threats to ME2.0 are similar to those of computing communication systems against CIA [142]. These threats result in direct PI leakages. ME2.0 communicates with services over Bluetooth without any reliance on Bluetooth security mechanism to deter eavesdropping attempts to compromise the transmissions confidentiality. ME2.0 own security and privacy mechanisms are utilised. A malicious entity modifying *meRequest* or *meReply* in unauthorised manners, violates the integrity of data. Availability is important for ubiquitous services to honour legitimate personalisation requests from users.

For users, the ability to access personalised services is also important. The availability might be threatened by malicious entities executing a distributed Denial of Service (DoS) on the service or overloading ME2.0 with unnecessary computations. These are direct threats to ME2.0 and are mitigated by the architectural design.

Impersonation or falsification threats in ME2.0 where a malicious entity attempts to mimic a legitimate service are countered by digital certificates issued by the CA and the enforced privacy policy as depicted in Figure 5.9.

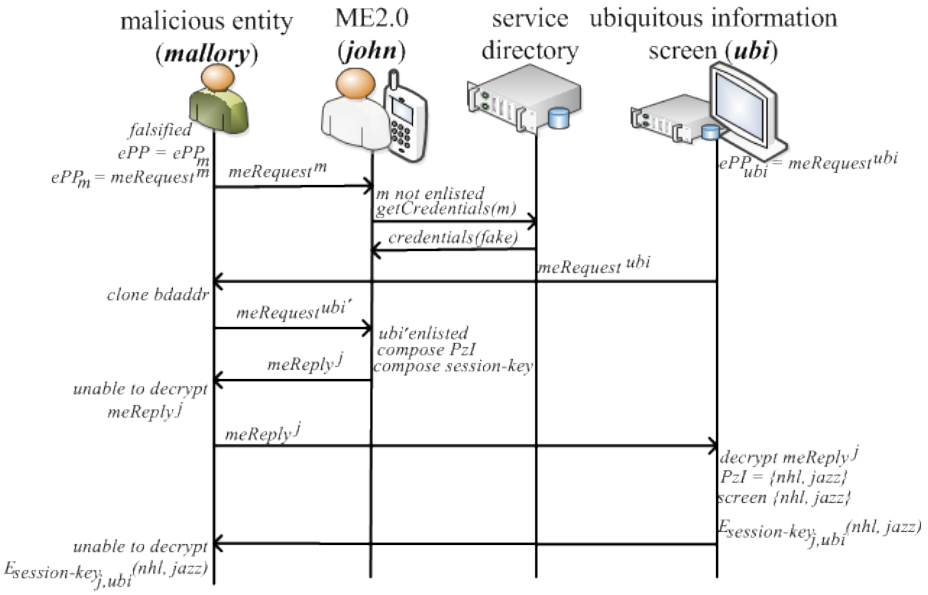



**Figure 5.9:** ME2.0 mitigation of impersonation.

It relatively easy for John to detect a fake $meRequest^m$ from Mallory, as they will not exist in his enlisted services, thus, prompting him to retrieve them from the service directory. In the service directory Mallory will be revealed as fake. If Mallory attempts to use a legitimate services enforced policy $meRequest^{ubi'}$ after cloning its *bdaddr*, that John has enlisted, the $meReply^j$ is encrypted with computed session-key from John's private-key and the services public-key based on the ECDH key exchange illustrated in Figure 3.7. Mallory lacks the information needed to compute the session-key or participate in the key-exchange, thus Mallory is unable to decrypt the content and determine John's disclosed PzI. If Mallory attempts to mimic John to the service he might be able to view John's personalised content on a ubiquitous screen. However, he will not be able to view the content on his mobile terminal as they are encrypted using the session-key which he lacks.

### 5.4.2 Indirect PI leaks

The disclosure of CnP by users rather than PzI and S/CI to ubiquitous services, mitigates a number of indirect leaks. The CnP in itself, limits the amount of users' data held by ubiquitous services. Enforced policies further regulate the amount of PzI services may

retrieve data by giving users some control of their disclosures. The disclosure policy allows users to articulate their privacy expectations clearly and restrict access to their PzI by simple changes in their disclosure policy. Privacy aspects regarding retention are declared in the disclosure policy as well. Unfortunately, the user lacks a mechanism to fully guarantee that services honour their handling expectations entirely. It is relatively easy for the service to indefinitely retain the PzI without the user ever knowing about it. To mitigate this, the best efforts are served by the EA.

The PRS adds an extra privacy insulation by isolating PzI and S/CI disclosures between users and the services they access. Mobile terminals can reserve battery or mitigate battery exhaustion attacks by using the PRS. Thus, the relocation of some computation might preserve ME2.0 battery as well as reinforcing the security. Additionally, mobile terminals are prone to theft or being misplaced. The relocation, of the more sensitive of portions of PzI limits the risks of their access by unauthorised individuals. The inbuilt two-factor authentication in ME2.0 mitigates and makes it more challenging to access users' PI. Similar to lost, misplaced or stolen keys and stolen credit cards, the user's swift action to change locks and cancel the cards are viable solutions. Similarly, changing S/KEY set is a viable solution for ME2.0.

The PRS has introduced new privacy threats by increasing the users' attack surface. Malicious entities need not only focus their attacks at mobile terminals and service providers, but also on the users' stationary PRS. The PRS also increases the time overhead on the ME2.0 scenario applicability. For instance, if a user walks by the information screen too quickly, or where there are numerous ME2.0 users interacting with the screen simultaneously, using different PRSs. This will impact the performance of the ubiquitous information screen. Adoption of multi-threaded agents in the service programming for interactions with mobile terminals and asynchronous interactions based on XML-RPC for interactions with users' PRS ensure that the entire service does not wait on a single ME2.0 instance. Rather other users continue to receive personalised services.

### 5.4.3 Enforcement and Enforcer Authority

In the context of this thesis, "enforcement" refers to the act of the EA binding valid certificates of a service to their privacy policy. Transforming the privacy policy to an enforced privacy policy, that is then published in a service directory permits users to download them to their mobile terminals and compare them with their own disclosure policies. Enforced policy results in an added layer of independent verification and validation of services. This works to the benefit of users. The advantage derived from the enforcement is directly attached to the selection of the EA. In communities where individuals trust their governments to protect and preserve their privacy, the government serves as a suitable EA. In contrasting regions where there is mutual distrust of local governments or suspicion of surveillance, a government based EA is unattractive to users. The role of EA is not to restrict what PzI the service may solicit or not. Rather, the EA binds whatever PzI the service intends to solicit from users and its promised processing of this information and hold the service accountable for meeting that obligation. Unannounced or after user complaint, the EA inspects what PzI the services are soliciting and whether they are processed in accordance to the stated promises. Services' enforced policies are published at the service directory in a manner that allows users to evaluate the services

privacy intentions, query, select a preferred service, and file complaints on any suspicion of misconduct.

The stages of enforcement of a certificate and privacy policy by an EA commence by the service provider first perform an ECDH [62] key-exchange to establish a shared secret-key over the insecure communication network. Then the service encrypts their privacy policy along with their signed credentials to the EA. The EA verifies and validates the authenticity of the provided credentials by contacting the mentioned CA. In the next the EA verifies whether the service has any pending or blacklisted enforced policy. If all stages are successful the privacy policy is enforced by inserting EA credentials, CA credentials and setting a validity period after which the newly composed policy is signed with ECDSA [62]. The enforced policy is published in the service directories for the service users to enlist. The services also use this enforced policy to simultaneously identify themselves to ME2.0 and solicit PzI.

Presentation of an enforced policy to ME2.0 triggers an authentication chain of activities that includes verifying the presented policy. This verification starts by the ME2.0 retrieving the EA's public-key either from its database repository or directly from the service directory. The public-key is used to verify the signature of enforced policy portion. If it passes the signature test and the digests are identical it is concluded that the enforced policy is authentic.

## 5.5 Discussions

This chapter has evaluated ME2.0 by first looking at important aspects that users associate with different features in software. The top 5 identified priorities for users are; stability, usability, functionalities, reliability, privacy and trust. From this list those closely related to this study are usability, security and privacy. These are used as the basis for evaluating ME2.0.

In the evaluation of ME2.0 usability; UI design prototyping, Internet-based surveys and wire-frame prototyping conducted with users have been published in [121]. The usability evaluation study revealed a number of users' insights, previously unconsidered and results in ME2.0 UI being completely seen from different user perspective that clearly has distinctions from previous UI.

The security and privacy evaluations considered how users disclose their PzI and still maintain their privacy in ME2.0. The mechanisms of authentication, cryptography and policy enforcements are discussed and the traditional cryptography ensuring CIA help in preserving direct PI leakages. Techniques involving CA, disclosure policies, and EA are instrumental in mitigating indirect PI leakages.

Finally, the implication of extra communication overheads due to security and privacy implementations were evaluated in [119]. The evaluation comprises the performance perspective of ME2.0. The PRS is also evaluated from a performance point of view. This chapter provides answers to the following part of the research question; *how can users organise and manage their PzI securely*?

Chapter VI

# Conclusions

This thesis has presented a solution that permits users to personalise ubiquitous services in which their Personal Information (PI) items are stored in their mobile terminals with privacy preserving capabilities. The PI items actively used to adapt the ubiquitous service's offerings to specific user preference are collectively termed Personalisation Information (PzI). The components of PzI include the user's Non-Personal or Group Identifiable Information (NP/GII), Personal or Group Preference (P/GPref) and their prevailing Situation or Context Information (S/CI).

To access personalised services, users are required to disclose portions of their PzI. A conflict exists between the users and the ubiquitous services they intend to access. While users seek to minimise their PzI disclosure to preserve their privacy, services are keen to maximise the solicitations of PzI in order to know their customers better. There is a limit at which services can no longer utilise all solicited PI for personalisation purposes. Excessive PI solicitations are likely to lead to infringement of users' Personal or Group Identifiable Information (P/GII), thereby exposing them to privacy compromises.

This thesis takes the user's perspective to solve this conflict, by evolving the Mobile Electronic Personality (ME) to its second generation, Mobile Electronic Personality Version 2 (ME2.0). The purpose of ME2.0 is to provide a mechanism for users to retain control over their PI in disclosures to access personalised ubiquitous services without leaking their PI items in the process.

The ME2.0 solution has demonstrated its advantages, in giving users more control over privacy decisions regarding the disclosure of their PzI to ubiquitous services matching or exceeding their privacy expectations in the handling of their PI. The main benefits to ME2.0 users are:

- An intuitively easy to use User Interface (UI) for configuring privacy expectations and disclosure policies. This resulted from involving users in the design and development process, leading eventually to fewer misconfigurations of privacy settings. Misconfigurations give users a false sense of security while indirectly leaking their PI.

- Users are better empowered to evaluate the privacy implications of disclosing particular PI to ubiquitous services in advance, and clearly articulate this decision in their disclosure policies.
- Permitting only strictly enforced ubiquitous service and redresses channels for users to report misconduct which limits risk taking services and inspires user confidence.
- Situations under which the PzI are provided to ubiquitous services are taken into account when adapting disclosures and limiting unexpected embarrassments.
- In ME2.0, unlike alternative personalisation techniques and technologies, users do not disclose their PI, Situation or Context Information and Personal or Group Preference. Rather, a user's S/CI is notated with their PI to determine the appropriate P/GPref to disclose, termed Context-Notated Preferences (CnP).
- ME2.0 is unlike privacy seals and symbols that lack guarantees, commitments and enforcement mechanisms. In ME services are independently verified and validated, with enforceable policies that not only provide redress channels for non-compliance complaints but also expose services to un-announced inspections.
- ME2.0 is useful in different situations where users' PI items are required. Beyond accessing and personalising ubiquitous services, it enables interactions with Service Accessing Device (SAD) and Service Accessing Application (SAA) to disclose PI items in the manual activities of filling in on-line forms.

The basic and extended functionalities of ME2.0 expose potentially new opportunities for ubiquitous service providers. For instance, retail stores providing a ubiquitous presence can be better aligned with the tastes or distaste of their target audience to improve their stock options and store atmosphere. Elderly citizens can inhabit more personalisation aware and conducive home with less privacy invasiveness.

Promises by services on their privacy practises and handling of users' PI, no longer need to be represented by signs, symbols or lengthy disclaimers that are user unfriendly and lack commitment in terms of enforcements. Instead users have at their disposal tangible controlling decisions at the users control that determine to whom their PzI are disclosed.

It is also ill-informed to assume that all ubiquitous services will always process user's PzI solicited through ME2.0 as specified in their privacy policies. The reasons for not following this policy option include the fact that firms change of ownerships or management. Legislations are also be amended from to time often to the potential detriment of the users PI privacy. The likelihood of unforeseen revenue streams in the future and absence of a fully viable means for users to determine what services deal with solicited PzI, motivates the continuity of the users and service struggle.

However, two useful steps to minimise privacy are presented. Firstly, by providing incentives for services to follow the policy and obtain valuable customers preferences. Secondly, through the existence of Enforcer Authority (EA) that ensures services behave appropriately on customers behalf. This study has made significant contributions towards preserving consumers' privacy by transparently limiting the disclosure of PzI and to services which it is disclosed.

## 6.1 Future work

The evolution of ME2.0 has detailed a number of usage scenarios which might prove useful in making the technology more user-friendly. Despite, the scenario postulations, these are merely experimental and conducted in controlled environments. There is a need to take ME2.0 out into real environments with real users and gain insights into its applicability. However, before this step can be taken, it should be evaluated on a real ubiquitous service infrastructure such as *http://ubioulu.fi/* and user defined PzI.

User defined personalisation is likely to increase the number and size of requests to services thereby slowing down the performance as they increase the execution load on mobile terminals. Researching possible solutions of this delay would be useful in the standardising the representation of PzI mark-up, perhaps with a preference mark-up language. This would ease the exchange of PzI between services as well as between ME2.0 enabled mobile terminals.

There are research benefits in further investigating the applicability of ME2.0 towards SAA and SAD domains. Numerous SAAs are emerging in the market and installed on mobile terminals using different information from different sources like sports-trackers and heart rate monitors, whose disclosures are unaccounted for. Having ME2.0 between these SAA and SAD would give users better control of their PI.

On the SADs front there are potential benefits to be realised, for instance, a desktop application for editing and entering PzI into ME2.0, enlisting ubiquitous services, as well as viewing ME2.0 logs would be beneficial to overcome the fact that mobile terminals have such a compact form.

[1] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, and P. Steggles. Towards a better understanding of context and context-awareness. In *Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing*, HUC '99, pages 304–307, London, UK, 1999. Springer-Verlag.

[2] G. D. Abowd, E. D. Mynatt, and T. Rodden. The human experience. *IEEE Pervasive Computing*, 1:48–57, January 2002.

[3] S. S. Al-Fedaghi. Personal management of private information. In *Innovations in Information Technology, 2006*, pages 1–5, nov. 2006.

[4] S. S. Al-Fedaghi. How sensitive is your personal information? In *Proceedings of the 2007 ACM symposium on Applied computing*, SAC '07, pages 165–169, New York, NY, USA, 2007. ACM.

[5] W. F. Alan. Privacy and freedom. volume 1. New York, 1967.

[6] M. Alia, V. S. Wold Eide, N. Paspallis, F. Eliassen, S. O. Hallsteinsen, and G. A. Papadopoulos. A utility-based adaptivity model for mobile applications. In *Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops - Volume 02*, AINAW '07, pages 556–563, Washington, DC, USA, 2007. IEEE Computer Society.

[7] T. Alvin. *Future Shock*. Random House, New York, 06 1970.

[8] G. Amato and U. Straccia. User profile modeling and applications to digital libraries. In *In: Proceedings of the Third European Conference on Research and Advanced Technology for Digital Libraries*, pages 184–197. Springer-Verlag, 1999.

[9] Amazon Corporation. amazon.com. http://www.amazon.com/, Accessed 14th November 2010.

[10] H. Ashman, T. Brailsford, and P. Brusilovsky. Personal services: Debating the wisdom of personalisation. In *Proceedings of the 8th International Conference on Advances in Web Based Learning*, ICWL '009, pages 1–11, Berlin, Heidelberg, 2009. Springer-Verlag.

[11] T. Aura. On the structure of delegation networks. In *Proc. 11th IEEE Computer Security Foundations Workshop*, pages 14–26, Rockport, MA, June 1998. IEEE Computer Society Press.

[12] N. F. Awad and Krishnan. The personalization privacy paradox: An empirical evaluation of information transparency and the willingeness to be profiled online for personalization. In *MIS Quarterly, (30: 1)*, 2006.

[13] L. Barkhuus and J. Tashiro. Student socialization in the age of facebook. In *Proceedings of the 28th international conference on Human factors in computing systems*, CHI '10, pages 133–142, New York, NY, USA, 2010. ACM.

[14] E. D. Bell and L. J. La-Padula. Secure computer systems: Mathematical foundations and model, November 1973.

[15] K.-I. Benta, A. Rarău, and M. Cremene. Ontology based affective context representation. In *Proceedings of the 2007 Euro American conference on Telematics and information systems*, EATIS '07, pages 46:1–46:9, New York, NY, USA, 2007. ACM.

[16] D. Benyon. Adaptive systems: A solution to usability problems. *User Modeling and User-Adapted Interaction*, 3:65–87, 1993. 10.1007/BF01099425.

[17] A. Beresford and F. Stajano. Location privacy in pervasive computing. *Pervasive Computing, IEEE*, 2(1):46–55, Jan-Mar 2003.

[18] C. Bettini, O. Brdiczka, K. Henricksen, J. Indulska, D. Nicklas, A. Ranganathan, and D. Riboni. A survey of context modelling and reasoning techniques. *Pervasive Mob. Comput.*, 6:161–180, April 2010.

[19] J. Bhattacharya, R. Dass, and V. K. S. K. Gupta. Utilizing network features for privacy violation detection. In *In Proc. of Int. Conf. on Communication System Software and Middleware*, 2006.

[20] I. F. Blake, G. Seroussi, and N. P. Smart. *Advances in Elliptic Curve Cryptography*, volume 1. Cambridge University Press., 2 edition, 2005.

[21] C. Boutilier, R. I. Brafman, H. H. Hoos, and D. Poole. Reasoning with conditional ceteris paribus preference statements. In *In Proceedings of the Fifteenth Conference on Uncertainty in Artificial Intelligence*, pages 71–80, 1999.

[22] B. Brumitt, B. Meyers, J. Krumm, A. Kern, and S. Shafer. Easyliving: Technologies for intelligent environments. In P. Thomas and H.-W. Gellersen, editors, *Handheld and Ubiquitous Computing*, volume 1927 of *Lecture Notes in Computer Science*, pages 97–119. Springer Berlin / Heidelberg, 2000. 10.1007/3-540-39959-3_2.

[23] B. Brumitt and S. Shafer. Better living through geometry. *Personal Ubiquitous Comput.*, 5(1):42–45, 2001.

[24] R. Burke. Hybrid recommender systems: Survey and experiments. *User Modeling and User-Adapted Interaction*, 12:331–370, November 2002.

[25] J. Carlisle. The privacy paradox. *Ubiquity*, 2002(April):1, 2002.

[26] D. L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24:84–90, February 1981.

[27] G. Chen and D. Kotz. A survey of context-aware mobile computing research. Technical report, Hanover, NH, USA, 2000.

[28] K. Cheverst, N. Davies, K. Mitchell, A. Friday, and C. Efstratiou. Developing a context-aware electronic tourist guide: some issues and experiences. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, CHI '00, pages 17–24, New York, NY, USA, 2000. ACM.

[29] Choice Stream. Personalisation survey of 2008. http://www.choicestream.com/pdf/ChoiceStream_2008_Personalization_Survey.pdf, Accessed 16.03.2010 2011.

[30] A. Civan, M. M. Skeels, A. Stolyar, and W. Pratt. Personal health information management: Consumers' perspectives.

[31] R. D. Cosmo. Educating the e-citizen. In *Proceedings of the 11th annual SIGCSE conference on Innovation and technology in computer science education*, ITICSE '06, pages 1–1, New York, NY, USA, 2006. ACM.

[32] M. desjardins. Dd-pref: A language for expressing preferences over sets. In *In AAAI-05*, 2005.

[33] M. desJardins, E. Eaton, and K. L. Wagstaff. Learning user preferences for sets of objects. In *Proceedings of the 23rd international conference on Machine learning*, ICML '06, pages 273–280, New York, NY, USA, 2006. ACM.

[34] A. K. Dey, G. D. Abowd, and D. Salber. A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications. *Hum.-Comput. Interact.*, 16:97–166, December 2001.

[35] M. Dideles. Bluetooth: A technical overview. *ACM Student*, 0(1), 2007.

[36] B. Dobbs, S. Egelman, G. Hogben, J. Humphrey, M. Langheinrich, and L. Cranor. Platform for privacy preferences 1.1 (p3p1.1). http://www.w3.org/TR/P3P11/, Accessed 16.03 2006.

[37] P. Dourish. What we talk about when we talk about context. *Personal Ubiquitous Computing.*, 8(1):19–30, 2004.

[38] e-Bay. http://www.ebay.com/, Accessed 12th November 2010.

[39] D. E. Eastlake. Electronic commerce modeling language (ecml) version 2 specification internet rfc 4115, June 2005.

[40] C. M. Ellison. Establishing identity without certification authorities. In *Proceedings of the 6th conference on USENIX Security Symposium, Focusing on Applications of Cryptography - Volume 6*, pages 7–7, Berkeley, CA, USA, 1996. USENIX Association.

[41] C. M. Ellison. The nature of a useable pki. *Computer Networks*, 31(8):823–830, 1999.

[42] C. M. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylönen. Spki certificate theory rfc2693. September 1999.

[43] T. Erickson. From pim to gim: personal information management in group contexts. *Commun. ACM*, 49:74–75, January 2006.

[44] R. Etter, P. D. Costa, and T. Broens. A rule-based approach towards context-aware user notification services. In *Proceedings of the 2006 ACS/IEEE International Conference on Pervasive Services*, pages 281–284, Washington, DC, USA, 2006. IEEE Computer Society.

[45] European Union. The european union data protection directive directive 95/46/ec. http://ec.europa.eu/justice/policies/privacy/, November 2010.

[46] R. Falkvinge. Sweden's new wiretapping law 'much worse than the stasi', http://thelocal.se/1234/20080610, Accessed 30th December 2011.

[47] E. Freeman and D. Gelernter. Lifestreams: a storage model for personal data. *SIGMOD Rec.*, 25:80–86, March 1996.

[48] E. Frias-martinez, G. Magoulas, S. Chen, and R. Macredie. Automated user modeling for personalized digital libraries. *International Journal of Information Management*, 26, 2006.

[49] B. C. M. Fung, M. Cao, B. C. Desai, and H. Xu. Privacy protection for rfid data. In *Proceedings of the 2009 ACM symposium on Applied Computing*, SAC '09, pages 1528–1535, New York, NY, USA, 2009. ACM.

[50] M. Gao, K. Liu, and Z. Wu. Personalisation in web computing and informatics: Theories, techniques, applications, and future research. *Information Systems Frontiers*, 12:607–629, November 2010.

[51] Gartner. Gartner identifies 10 consumer mobile applications to watch in 2012. http://www.gartner.com/it/page.jsp?id=1544815, 2010, Accessed 11th November 2010.

[52] Gartner. Mobile applications store revenue forecast to reach $17.7 billion in 2011. http://www.gartner.com/it/page.jsp?id=1529214, 2010, Accessed 11th November 2010.

[53] C. Gena. Evaluation methodologies and user involvement in user, 2003.

[54] M. Goel and S. Sarkar. Web site personalization using user profile information. In *Proceedings of the Second International Conference on Adaptive Hypermedia and Adaptive Web-Based Systems*, AH '02, pages 510–513, London, UK, UK, 2002. Springer-Verlag.

[55] Google. http://www.google.com/, 2010, Accessed 11th November.

[56] A. Goy, L. Ardissono, and G. Petrone. The adaptive web. chapter Personalization in e-commerce applications, pages 485–520. Springer-Verlag, Berlin, Heidelberg, 2007.

[57] F. Granelli, H. Zhang, X. Zhou, and S. Maranò. Research advances in cognitive ultra wide band radio and their application to sensor networks. *Mob. Netw. Appl.*, 11:487–499, August 2006.

[58] T. Gross and M. Specht. Awareness in context-aware information systems, 2001.

[59] V. Gupta, S. Gupta, S. Chang, and D. Stebila. Performance analysis of elliptic curve cryptography for ssl. In *Proceedings of the 1st ACM workshop on Wireless security*, WiSE '02, pages 87–94, New York, NY, USA, 2002. ACM.

[60] S. Hada, G. Powers, C. Schunter, and P. Ashley. Enterprise privacy authorisation language (epal). http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/, Accessed 16.03.2011 2003.

[61] S. Hallsteinsen, E. Stav, and J. Floch. Self-adaptation for everyday systems. In *WOSS '04: Proceedings of the 1st ACM SIGSOFT workshop on Self-managed systems*, pages 69–74, New York, NY, USA, 2004. ACM.

[62] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer-Verlag New York, Inc, 2004.

[63] C. Hayes. Hackers take down fine gael website and compromise privacy of 4000 public users. http://www.irishcentral.com/news/Hackers-take-down-Fine-Gael-website-and-compromise-privacy-of-4000-public-users-113195684.html, Accessed 11th November 2010.

[64] Helsinki Times. Lex nokia gets blessings from constitutional law committee', http://hs.fi/english/lex-nokia-gets-blessing-from-constitutional-law committee/113524092046, Accessed 30th December 2011.

[65] K. Henricksen, J. Indulska, and A. Rakotonirainy. Modeling context information in pervasive computing systems. In *Proceedings of the First International Conference on Pervasive Computing*, Pervasive '02, pages 167–180, London, UK, 2002. Springer-Verlag.

[66] A. S. Hornby. *Oxford Advanced Learners Dictionary of Current English*, volume 1 of *1*. Oxford University Press, 5 edition, 1995.

[67] I. Horrocks, P. F. Patel-Schneider, and F. van Harmelen. From shiq and rdf to owl: the making of a web ontology language. *Web Semantics: Science, Services and Agents on the World Wide Web*, 1(1):7–26, 2003.

[68] IEEE. Ieee standards association, http://standards.ieee.org/about/get/802/802.11.html, Accessed 30th December 2011.

[69] ISO 7498-2. Information processing system - open system interconnection - basic reference model - part 2: security architecture, 1989.

[70] A. Jääskeläinen and K. Heikkinen. Divergence of user experience: Professionals vs. end users. *In proceedings of I-UxSED 2010*, 30, October 2010.

[71] P. Jäppinen. *Mobile Electronic Personality*. PhD thesis, Lappeenranta University Of Technology, 2004.

[72] P. Jäppinen and J. Porras. Analyzing the attributes of personalization information affecting storage location. In *International Conference on E-Society*. IADIS, June 2003.

[73] P. Jarvinen. *On Research methods*, volume 1 of *1*. Opinpajan Kirja, 1 edition, July 2004.

[74] K. Heikkinen, J. Eerola, P. Jäppinen, J. Porras. Personalized view of personal information. *WSEAS, Transactions on information science and applications, Vol 2, No. 4, 2004.*, April 2004.

[75] Kantara. Kantara initiative. http://kantarainitiative.org/, Accessed 16.03 2011.

[76] A. Kobsa and W. Wahlster, editors. *User models in dialog systems*. Springer-Verlag New York, Inc., New York, NY, USA, 1989.

[77] G. Koch, U. Kebschull, and W. Rosenstiel. A prototyping environment for hardware/software codesign in the cobra project. In *Proceedings of the 3rd international workshop on Hardware/software co-design*, CODES '94, pages 10–16, Los Alamitos, CA, USA, 1994. IEEE Computer Society Press.

[78] K. Kodama, Y. Iijima, X. Guo, and Y. Ishikawa. Skyline queries based on user locations and preferences for making location-based recommendations. In *Proceedings of the 2009 International Workshop on Location Based Social Networks*, LBSN '09, pages 9–16, New York, NY, USA, 2009. ACM.

[79] B. Könings, B. Wiedersheim, and M. Weber. Privacy management and control in atraco. In *Proceedings of the First international joint conference on Ambient intelligence*, AmI'10, pages 51–60, Berlin, Heidelberg, 2010. Springer-Verlag.

[80] Korfhage and R. R. Query enhancement by user profiles. In *Proc. of the third joint BCS and ACM symposium on Research and development in information retrieval*, pages 111–121, New York, NY, USA, 1984. Cambridge University Press.

[81] R. Kraemer and P. Schwander. Bluetooth based wireless internet applications for indoor hot spots: experience of a successful experiment during cebit 2001. *Comput. Netw.*, 41:303–312, February 2003.

[82] Kuhf.fm. Ipv6: smartphone compromise users privacy. http://thenetworkworld.blogspot.com/2011/01/ipv6-smartphones-compromise-users.html, Accessed 11th November 2010.

[83] Y.-F. Kuo and L.-S. Chen. Personalization technology application to internet content provider. *Expert Syst. Appl.*, 21(4):203–215, 2001.

[84] M. Lamming and M. Flynn. Forget-me-not: Intimate computing in support of human memory. pages 125–128, 1994.

[85] L. Lamport. Password authentication with insecure communication. *Commun. ACM*, 24:770–772, November 1981.

[86] R. LaRose and N. Rifon. Your privacy is assured-of being invaded. web sites with and without privacy seals https://www.msu.edu/ larose/es2003post.htm march 2003. Accessed 4th February 2010.

[87] S. Latanya. k-anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness Knowledge Based Systems.*, 10:557–570, October 2002.

[88] S.-Y. Lau, T.-H. Chang, S.-Y. Hu, H.-J. Huang, L. de Shyu, C.-M. Chiu, and P. Huang. Sensor networks for everyday use: The bl-live experience. *Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on*, 1:336–343, June 2006.

[89] S. Lederer, I. Hong, K. Dey, and A. Landay. Personal privacy through understanding and action: five pitfalls for designers. *Personal Ubiquitous Comput.*, 8(6):440–454, 2004.

[90] T.-P. Liang, Y.-F. Yang, D.-N. Chen, and Y.-C. Ku. A semantic-expansion approach to personalized knowledge recommendation. *Decis. Support Syst.*, 45:401–412, June 2008.

[91] Liberty Alliance. Project liberty alliance. http://www.projectliberty.org/, Accessed 16 May 2011.

[92] K. B. Limon and P. B. Hill. Microsoft .net passport and wallet: Approach with caution!, http://web.mit.educ/is/isnews/v17/n04/170408.html, Accessed 30th November 2011.

[93] H. Liu, B. Salem, Rauterberg, and Matthias. Adaptive user preference modeling and its application to in-flight entertainment. In *Proceedings of the 3rd international conference on Digital Interactive Media in Entertainment and Arts*, DIMEA '08, pages 289–294, New York, NY, USA, 2008. ACM.

[94] J. Lumsden and L. MacKay. How does personality affect trust in b2c e-commerce? In *Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet*, ICEC '06, pages 471–481, New York, NY, USA, 2006. ACM.

[95] J.-F. Mainguet. Fingerprint fake detection. In S. Z. Li and A. Jain, editors, *Encyclopedia of Biometrics*, pages 458–465. Springer US, 2009.

[96] E. Mayberry. Facebook connected smartphones can compromise privacy. http://app1.kuhf.org/articles/1298078472-Facebook-Connected-Smartphones-Can-Compromise-Privacy.html/, Accessed 11th November 2010.

[97] R. Mayrhofer. An architecture for context prediction. In *In Advances in Pervasive Computing, number 3-85403-176-9. Austrian Computer Society (OCG*, 2004.

[98] U. M. Mbanaso, G. S. Cooper, D. W. Chadwick, and S. Proctor. Privacy preserving trust authorization framework using xacml. In *WOWMOM '06: Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks*, pages 673–678, Washington, DC, USA, 2006. IEEE Computer Society.

[99] Microsoft. Sketchflow. http://www.microsoft.com/expression/products/, Accessed 12th November 2010.

[100] Microsoft Corporation. Windows card space. http://www.microsoft.com/windows/products/winfamily/cardspace/, Accessed 16.03 2011.

[101] Microsoft Corporation. Windows live id. http://windows.microsoft.com/en-US/windows7/what-is-a-windows-live-id, Accessed 16.03 2011.

[102] C. J. Mitchell and L. Chen. Comments on the s/key user authentication scheme. *SIGOPS Oper. Syst. Rev.*, 30:12–16, October 1996.

[103] T. T. Moores and G. Dhillon. Do privacy seals in e-commerce really work? *Commun. ACM*, 46(12):265–271, 2003.

[104] H. Mukhtar, D. Belaïd, and G. Bernard. A quantitative model for user preferences based on qualitative specifications. In *Proceedings of the 2009 international conference on Pervasive services*, ICPS '09, pages 179–188, New York, NY, USA, 2009. ACM.

[105] H. Mukhtar, D. Belaïd, and G. Bernard. Session continuity and splitting of multimedia applications using qualitative user preferences. In *Proceedings of the 6th International Conference on Mobile Technology, Application & Systems*, Mobility '09, pages 52:1–52:8, New York, NY, USA, 2009. ACM.

[106] H. Mukhtar, D. Belaïd, and G. Bernard. Dynamic user task composition based on user preferences. *ACM Trans. Auton. Adapt. Syst.*, 6:4:1–4:17, February 2011.

[107] G. Mulligan. The 6lowpan architecture. In *Proceedings of the 4th workshop on Embedded networked sensors*, EmNets '07, pages 78–82, New York, NY, USA, 2007. ACM.

[108] Q. Ni, A. Trombetta, E. Bertino, and J. Lobo. Privacy-aware role based access control. In *Proceedings of the 12th ACM symposium on Access control models and technologies*, SACMAT '07, pages 41–50, New York, NY, USA, 2007. ACM.

[109] NIST. Guide to protecting the confidentiality of personal identifiable information (pii). http://csrc.nist.gov/publications/nistpubs/800 122/sp800 122.pdf, Accessed 16.03 2011.

[110] Nokia Corporation. Symbian s60 module reference - e32db interface to the symbian native db. http://pys60.garage.maemo.org/doc/s60/module-e32db.html, Accessed 24th June 2010.

[111] Nokia Corporation. Symbian s60 module reference - e32dbm dbm implemented using the symbian native dbms. http://pys60.garage.maemo.org/doc/s60/module-e32dbm.html, Accessed 24th June 2010.

[112] Nokia Develper. Device details, http://develper.com/devices/device_specifications/, Accessed 30th December 2011.

[113] P. A. Norberg, D. R. Horne, and D. A. Horne. The privacy paradox: Personal information disclosure intentions versus behaviours. *Journal of Consumer Affairs*, 41(1):100–126, 2007.

[114] OpenID. Opend id single sign on. http://openid.net/get-an-openid/ what-is-openid/, Accessed 16.03 2011.

[115] G. Orwell. *Nineteen eighty-four*, volume 1. New York : Harcourt, Brace, [c1949]., 2 edition, 1949.

[116] W. Oyomno and P. Jäppinen. Security and privacy in a ubiquitous information screen. *7th Minema Workshop, WAWC08 confrence.*, (2):133–143, 2008.

[117] W. Oyomno, P. Jäppinen, and E. Kerttula. Privacy implications of context-aware services. In *COMSWARE '09: Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middlewaRE*, pages 1–9, New York, NY, USA, 2009. ACM.

[118] W. Oyomno, P. Jäppinen, and E. Kerttula. Privacy policy enforcement for ambient ubiquitous services. In *Ambient Intelligence*, volume 6439 of *Lecture Notes in Computer Science*, pages 265–269. Springer Berlin / Heidelberg, 2010. 10.1007/978-3-642-16917-5_28.

[119] W. Oyomno, P. Jäppinen, and E. Kerttula. Privacy preserving architecture for context-enhanced personalised pervasive screens. *Pervasive2010 workshop on pervasive advertising and shopping*, 8(5):569–587, 2010.

[120] W. Oyomno, P. Jäppinen, and E. Kerttula. Privacy preservation for personalised services in smart spaces. Baltic Conference on Future Internet Communications, Riga, Latvia, 2011.

[121] W. Oyomno, P. Jäppinen, E. Kerttula, and K. Heikkinen. Usability study of me2.0. *Personal and Ubiquitous Computing*, pages 1–15. 10.1007/s00779-011-0495-9.

[122] P. Hough. Bluetooth specification version 3.0+hs[vol 0], https://bluetooth.org/technical/specifications/adopted.htm, Accessed 30th December 2011.

[123] W. Park, L. Jones, and G. Robinson. Bluetooth specification version 2.1 + edr. *Bluetooth SIG*, 0(2.1):1–1420, 2007.

[124] J. Pascoe. Adding generic contextual capabilities to wearable computers. In *Wearable Computers, 1998. Digest of Papers. Second International Symposium on*, pages 92–99, oct 1998.

[125] J. Pascoe, N. Ryan, and D. Morse. Issues in developing context-aware computing. In H.-W. Gellersen, editor, *Handheld and Ubiquitous Computing*, volume 1707 of *Lecture Notes in Computer Science*, pages 208–221. Springer Berlin / Heidelberg, 1999. 10.1007/3-540-48157-5_20.

[126] E. Pérez, A. Fortier, G. Rossi, and S. Gordillo. Rethinking context models. In *Proceedings of the Confederated International Workshops and Posters On the Move to Meaningful Internet Systems: ADI, CAMS, EI2N, ISDE, IWSSA, MONET, On To Content, ODIS, ORM, OTM Academy, SWWS, SEMELS, Beyond SAWSDL, and COMBEK 2009*, OTM '09, pages 78–87, Berlin, Heidelberg, 2009. Springer-Verlag.

[127] S. Perugini and N. Ramakrishnan. Personalizing web sites with mixed-initiative interaction. *IT Professional*, 5:9–15, March 2003.

[128] C. Pfleeger and S. L. Pfleeger. *Security in computing*, volume 1. Prentice hall, 1 edition, 2003.

[129] D. Piasecki. Rfid update: The basics, the wal-mart mandate, epc, privacy concerns, and more., Accessed 11th November 2010.

[130] F. Rahman, M. E. Hoque, F. A. Kawsar, and S. I. Ahamed. Preserve your privacy with pco: A privacy sensitive architecture for context obfuscation for pervasive e-community based applications. In *Proceedings of the 2010 IEEE Second International Conference on Social Computing*, SOCIALCOM '10, pages 41–48, Washington, DC, USA, 2010. IEEE Computer Society.

[131] P. Rossel and M. Finger. Conceptualizing e-governance. In *Proceedings of the 1st international conference on Theory and practice of electronic governance*, ICEGOV '07, pages 399–407, New York, NY, USA, 2007. ACM.

[132] S. Hall. Bluetooth specification version 2.0+edr, https://bluetooth.org/technical/specifications/adopted.htm, Accessed 30th December 2011.

[133] S. Saklikar and S. Saha. Next steps for security assertion markup language (saml). In *SWS '07: Proceedings of the 2007 ACM workshop on Secure web services*, pages 52–65, New York, NY, USA, 2007. ACM.

[134] Samsung Electronics. Samsung galaxy s ii gt-i9100, http://samsung.com/uk/consumer/mobile-devices/smartphones/android/gt-i9100lkaxeu-specsa/, Accessed 30th December 2011.

[135] B. Schilit, N. Adams, and R. Want. Context-aware computing applications. In *Mobile Computing Systems and Applications, 1994. Proceedings., Workshop on*, pages 85–90, dec 1994.

[136] B. Schilit and M. Theimer. Disseminating active map information to mobile hosts. *IEEE Network*, 8:22–32, 1994.

[137] B. Schneier. *Applied cryptography, Protocols, algorithms and source code in C*, volume 1. John Wiley and Sons, Inc, 2 edition, 1996.

[138] J. Schreier. Sony scrambles after 'external intrusion' takes down playstation network. http://www.wired.com/gamelife/2011/04/psn-down/, Accessed 11th November 2010.

[139] M. Shopov, G. Spasov, and G. Petrova. Architectural models for realization of web-based personal health systems. In *Proceedings of the International Conference on Computer Systems and Technologies and Workshop for PhD Students in Computing*, CompSysTech '09, pages 53:1–53:6, New York, NY, USA, 2009. ACM.

[140] S. Speilberg, G. Molen, W. Parkes, J. de Bont, and M. Doven. Minority report, June 2002.

[141] Sqlite 3. Sqlite3 database. http://www.sqlite.org/, Accessed 10th November 2010.

[142] F. Stajano. *Security for Ubiquitous Computing*. John Wiley and Sons, Febuary 2002.

[143] L. A. Suchman. *Plans and situated actions: the problem of human-machine communication*. Cambridge University Press, New York, NY, USA, 1987.

[144] The ZigBee Alliance. Zigbee. http://www.zigbee.org/en/resources/analystreports.asp, Accessed 24th June 2010.

[145] R. G. Tiwari, M. Husain, V. Srivastava, and K. Singh. A hypercube novelty model for comparing e-commerce and m-commerce. In *Proceedings of the 2011 International Conference on Communication, Computing & Security*, ICCCS '11, pages 616–619, New York, NY, USA, 2011. ACM.

[146] S. I. Wains and W. Mahmood. Integrating m-learning with e-learning. In *Proceedings of the 9th ACM SIGITE conference on Information technology education*, SIGITE '08, pages 31–38, New York, NY, USA, 2008. ACM.

[147] V. J. Waldo, H. S. Lin, and L. I. Miller. *Engaging privacy and information technology in a digital age*, volume 1. National Academy Press, 1 edition, 2007.

[148] A. Ward and A. Jones. A new location technique for the active office, 1997.

[149] Webropol. Webropol. http://w3.webropol.com/, 2010, Accessed 4th April 2010.

[150] M. Weiser. The computer for the 21st century. In *Scientific American Journal*, pages 94–104, New York, NY, USA, 1991. ACM.

[151] M. Weller. *Virtual Learning Environments: Using, Choosing and Developing your VLE*. Routledge, Oxford, UK, February 2007.

[152] R. Wishart, K. Henricksen, and J. Indulska. Context obfuscation for privacy via ontological descriptions, 2005.

[153] J. Xu, C. Jiang, A. Guo, Y. Hong, S. Li, and X. Bai. Lower bounds on lifetime of ultra wide band wireless sensor networks. *Wirel. Netw.*, 16:1739–1748, August 2010.

[154] N. Xu, F. Zhang, Y. Luo, W. Jia, D. Xuan, and J. Teng. Stealthy video capturer: a new video-based spyware in 3g smartphones. In *Proceedings of the second ACM conference on Wireless network security*, WiSec '09, pages 69–78, New York, NY, USA, 2009. ACM.

[155] C. Zhai, W. W. Cohen, and J. Lafferty. Beyond independent relevance: Methods and evaluation metrics for subtopic retrieval. In *In Proceedings of SIGIR*, pages 10–17, 2003.

[156] A. Zimmermann, M. Specht, and A. Lorenz. Personalization and context management. *User Modeling and User-Adapted Interaction*, 15:275–302, August 2005.

Appendix I

# ME2.0 Request and response mark-ups

## I.1 Request Extensible Mark-up Language (XML) schema

**Listing I.1:** Request XML schema

```
<?xml version="1.0" encoding="utf-8">
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="me_request">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="credential">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="serviceName" type="xs:string"/>
            <xs:element name="sphere" type="xs:string"/>
            <xs:element name="valid" type="xs:dateTime"/>
            <xs:element name="category" type="xs:string"/>
            <xs:element name="description" type="xs:string"/>
            <xs:element name="owner" type="xs:string"/>
            <xs:element name="bdaddr" type="xs:string"/>
            <xs:element name="ciphers">
              <xs:complexType>
                <xs:sequence>
                  <xs:element name="ecc">
                    <xs:complexType>
                      <xs:sequence>
                        <xs:element name="parameters" type="xs:string"/>
                        <xs:element name="eccPkey" type="xs:string"/>
                      </xs:sequence>
                    </xs:complexType>
                  </xs:element>
                  <xs:element name="x509">
                    <xs:complexType>
                      <xs:sequence>
                        <xs:element name="certifier" type="xs:string"/>
                        <xs:element name="signature" type="xs:string"/>
                      </xs:sequence>
                    </xs:complexType>
```

```
                </xs:element>
                <xs:element name="ea">
                  <xs:complexType>
                    <xs:sequence>
                      <xs:element name="enforcer" type="xs:string"/>
                      <xs:element name="signature" type="xs:string"/>
                    </xs:sequence>
                  </xs:complexType>
                </xs:element>
              </xs:complexType>
            </xs:element>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="request" minOccurs="1" maxOccurs="unbounded">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="item" type="xs:string"/>
            <xs:element name="aim" type="xs:string"/>
            <xs:element name="kept" type="xs:nonNegativeInteger"/>
            <xs:element name="oblige" type="xs:boolean"/>
            <xs:element name="seclev">
              <xs:restriction base="xs:string">
                <xs:enumeration value="public"/>
                <xs:enumeration value="restricted"/>
                <xs:enumeration value="confidential"/>
                <xs:enumeration value="secret"/>
                <xs:enumeration value="top_secret"/>
              </xs:restriction>
            </xs:element>
            <xs:element name="share" type="xs:string" minOccurs="0"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
</xs:schema>
```

## I.2 Reply XML schema

**Listing I.2:** Request XML schema

```
<?xml version="1.0" encoding="utf-8">
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="me_reply">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="credential">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="serviceName" type="xs:string"/>
            <xs:element name="ciphers">
              <xs:complexType>
                <xs:sequence>
                  <xs:element name="ecc">
                    <xs:complexType>
                      <xs:sequence>
                        <xs:element name="parameters" type="xs:string"/>
                        <xs:element name="eccPkey" type="xs:string"/>
                      </xs:sequence>
                    </xs:complexType>
                  </xs:element>
                </xs:sequence>
              </xs:complexType>
            </xs:element>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="reply" minOccurs="1" maxOccurs="unbounded">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="item" type="xs:string"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
</xs:schema>
```

# Frequency of user responses

**Table II.1:** Frequency of user responses on importance attached to features

| Features | Frequency of responses | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | Weighted mean |
| accessibility | 515 | 622 | 142 | 24 | 7 | 50 | 1.92 |
| aesthetics | 72 | 343 | 497 | 165 | 35 | 232 | 3.33 |
| brand | 17 | 121 | 336 | 537 | 328 | 13 | 3.79 |
| consistency | 470 | 568 | 177 | 23 | 8 | 101 | 2.13 |
| coolness | 43 | 176 | 421 | 457 | 244 | 18 | 3.54 |
| device | 138 | 484 | 444 | 206 | 48 | 42 | 2.75 |
| own emotions | 88 | 353 | 464 | 318 | 112 | 25 | 3.06 |
| use environment | 60 | 329 | 507 | 348 | 93 | 24 | 3.12 |
| own expectations | 101 | 493 | 512 | 199 | 31 | 20 | 2.72 |
| functionalities | 835 | 424 | 76 | 12 | 2 | 11 | 1.49 |
| interaction | 272 | 526 | 391 | 105 | 15 | 44 | 2.41 |
| own motivation | 214 | 502 | 471 | 125 | 24 | 25 | 2.50 |
| pleasure | 148 | 500 | 463 | 182 | 40 | 27 | 2.67 |
| price of purchase | 347 | 490 | 314 | 133 | 50 | 27 | 2.36 |
| reliability | 849 | 387 | 80 | 17 | 4 | 20 | 1.52 |
| stability | 995 | 307 | 43 | 7 | 2 | 7 | 1.34 |
| trust and privacy | 738 | 461 | 124 | 26 | 5 | 7 | 1.60 |
| usability | 834 | 444 | 57 | 2 | 2 | 15 | 1.48 |
| usefulness | 563 | 510 | 186 | 49 | 21 | 24 | 1.88 |
| user interface | 315 | 600 | 266 | 43 | 12 | 116 | 2.40 |
| ease of taking into use | 433 | 552 | 276 | 72 | 11 | 12 | 2.05 |

Appendix III

# Internet-based survey


**Figure III.1:** Internet-based survey page 1.

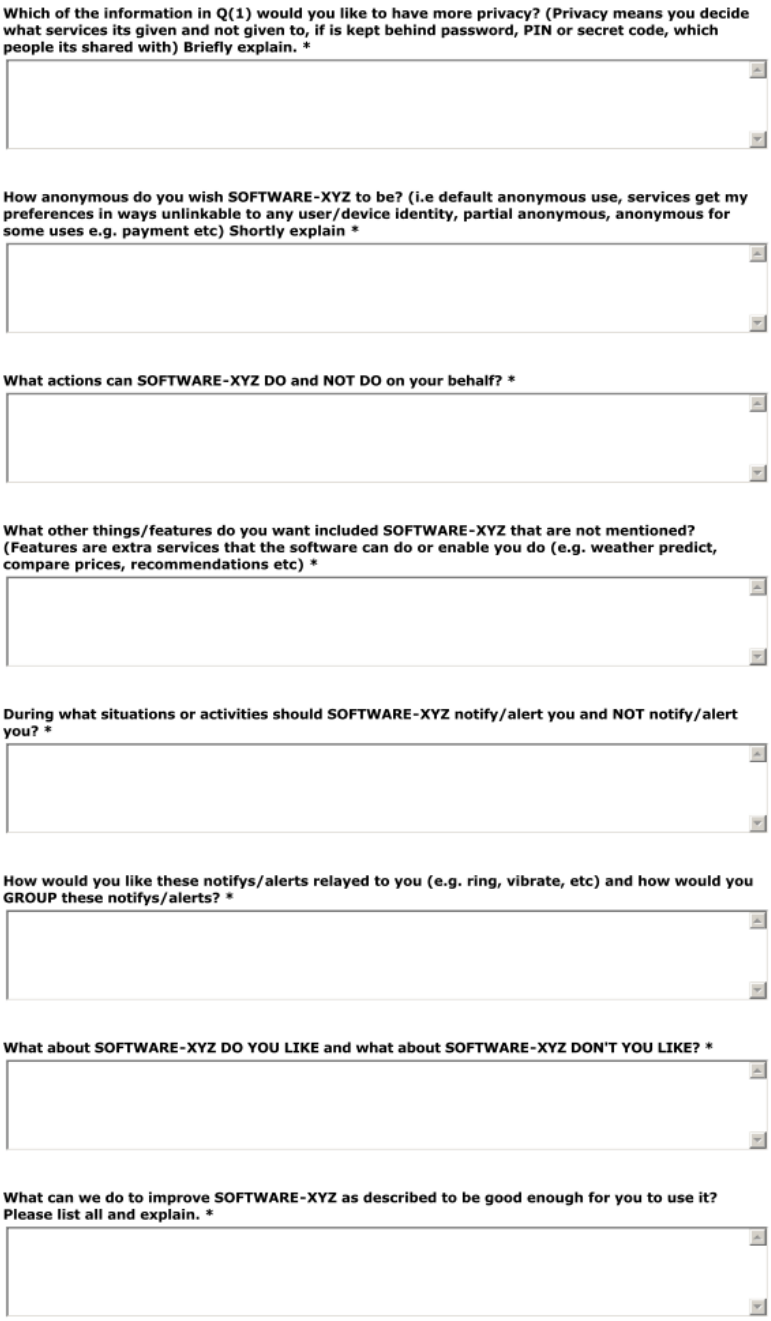
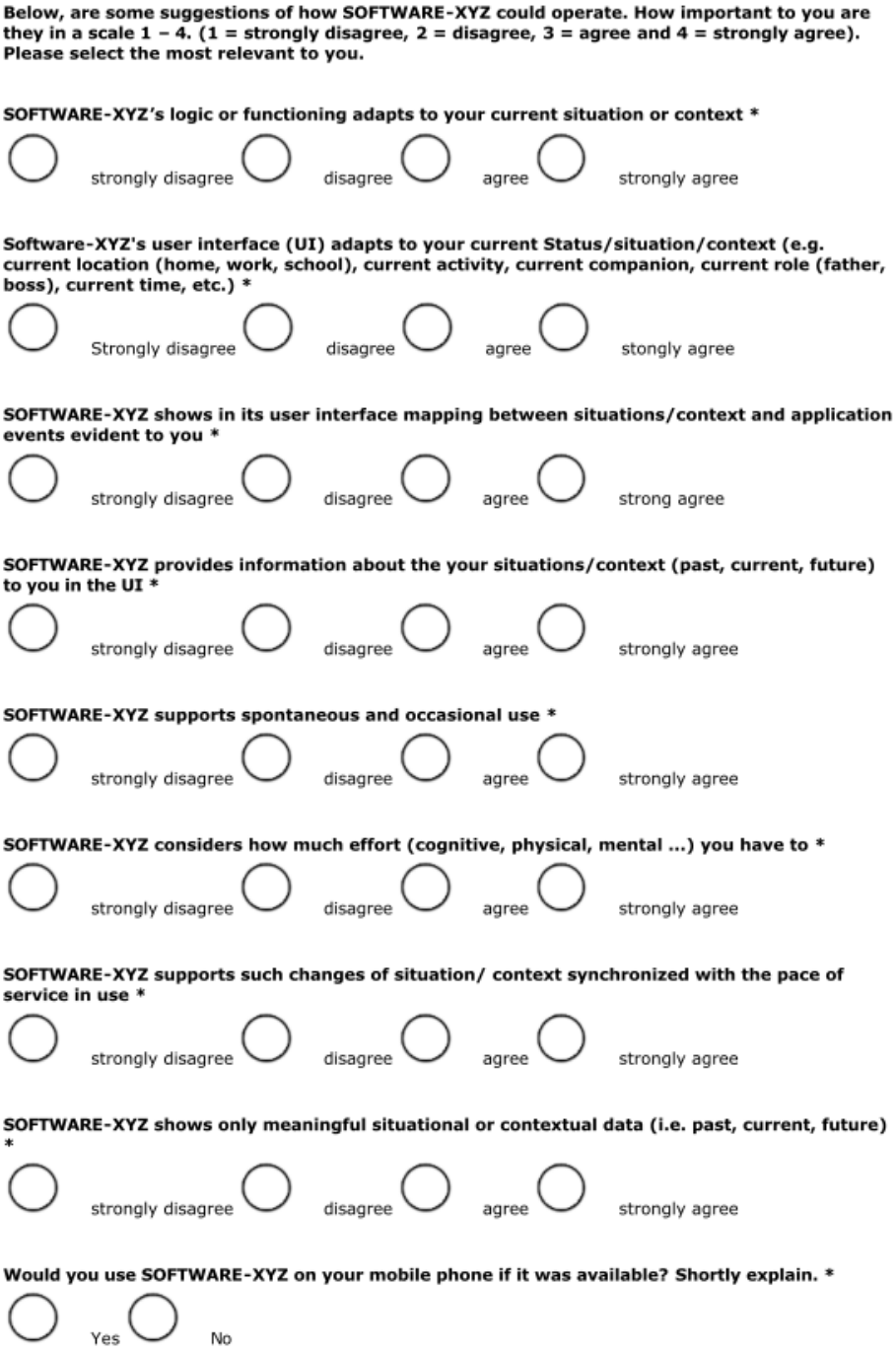



**Figure III.2:** Continuation of Page 1.



**Below, are some suggestions of how SOFTWARE-XYZ could operate. How important to you are they in a scale 1 – 4. (1 = strongly disagree, 2 = disagree, 3 = agree and 4 = strongly agree). Please select the most relevant to you.**

**SOFTWARE-XYZ's logic or functioning adapts to your current situation or context ***

strongly disagree disagree agree strongly agree

**Software-XYZ's user interface (UI) adapts to your current Status/situation/context (e.g. current location (home, work, school), current activity, current companion, current role (father, boss), current time, etc.) ***

Strongly disagree disagree agree stongly agree

**SOFTWARE-XYZ shows in its user interface mapping between situations/context and application events evident to you ***

strongly disagree disagree agree strong agree

**SOFTWARE-XYZ provides information about the your situations/context (past, current, future) to you in the UI ***

strongly disagree disagree agree strongly agree

**SOFTWARE-XYZ supports spontaneous and occasional use ***

strongly disagree disagree agree strongly agree

**SOFTWARE-XYZ considers how much effort (cognitive, physical, mental ...) you have to ***

strongly disagree disagree agree strongly agree

**SOFTWARE-XYZ supports such changes of situation/ context synchronized with the pace of service in use ***

strongly disagree disagree agree strongly agree

**SOFTWARE-XYZ shows only meaningful situational or contextual data (i.e. past, current, future) ***

strongly disagree disagree agree strongly agree

**Would you use SOFTWARE-XYZ on your mobile phone if it was available? Shortly explain. ***

Yes No

**Figure III.3:** Internet-based survey page 2.

**Age group ***

16-20 21-25 26-30 31-35 36-40

41-45 46-50 51-55 56-60 61-65

66+

**Gender ***

Female Male

**What is your profession? (i.e. industry / field of expertise) ***

**What is your current location? (Country, City)**

**How many mobile phones do you own? ***

0-1 2-3 4-5 6-7 8+

**Do you use internet on your phone(s) and what for? (e.g. email, facebook, twitter, spotify, dropbox, remote desktop etc. ***

Yes No

**If you answered Yes to previous Question please list the services you use. If you answered No shortly explain your reasons for not using internet on your phone(s). ***

**Rate your computer / Information technology skills ***

Unskilled skilled Somewhat Skilled skilled Very skilled Extremly

**Figure III.4:** Internet-based survey page 3.

**ACTA UNIVERSITATIS LAPPEENRANTAENSIS**

**437.** REPO, EVELIINA. EDTA- and DTPA-functionalized silica gel and chitosan adsorbents for the removal of heavy metals from aqueous solutions. 2011. Diss.

**438.** PODMETINA, DARIA. Innovation and internationalization in Russian companies: challenges and opportunities of open innovation and cooperation. 2011. Diss.

**439.** SAVITSKAYA, IRINA. Environmental influences on the adoption of open innovation: analysis of structural, institutional and cultural impacts. 2011. Diss.

**440.** BALANDIN, SERGEY, KOUCHERYAVY, YEVGENI, JÄPPINEN, PEKKA, eds. Selected Papers from FRUCT 8 .2011.

**441.** LAHTI, MATTI. Atomic level phenomena on transition metal surfaces. 2011. Diss.

**442.** PAKARINEN, JOUNI. Recovery and refining of manganese as by-product from hydrometallurgical processes. 2011. Diss.

**443.** KASURINEN, JUSSI. Software test process development. 2011. Diss.

**444.** PEKKANEN, PETRA. Delay reduction in courts of justice – possibilities and challenges of process improvement in professional public organizations. 2011. Diss.

**445.** VANHALA, MIKA. Impersonal trust within the organization: what, how, and why? 2011. Diss.

**446.** HYNYNEN, KATJA. Broadband excitation in the system identification of active magnetic bearing rotor systems. 2011. Diss.

**447.** SOLONEN, ANTTI. Bayesian methods for estimation, optimization and experimental design. 2011. Diss.

**448.** JABLONSKA, MATYLDA. From fluid dynamics to human psychology. What drives financial markets towards extreme events. 2011. Diss.

**449.** MYÖHÄNEN, KARI. Modelling of combustion and sorbent reactions in three-dimensional flow environment of a circulating fluidized bed furnace. 2011. Diss.

**450.** LAATIKAINEN, MARKKU. Modeling of electrolyte sorption – from phase equilibria to dynamic separation systems. 2011. Diss.

**451.** MIELONEN, JARI. Making Sense of Shared Leadership. A case study of leadership processes and practices without formal leadership structure in the team context. 2011. Diss.

**452.** PHAM, ANH TUAN. Sewage sludge electro-dewatering. 2011. Diss.

**453.** HENNALA, LEA. Kuulla vai kuunnella – käyttäjää osallistavan palveluinnovoinnin lähestymistavan haasteet julkisella sektorilla. 2011. Diss.

**454.** HEINIMÖ, JUSSI. Developing markets of energy biomass – local and global perspectives. 2011. Diss.

**455.** HUJALA, MAIJA. Structural dynamics in global pulp and paper industry. 2011. Diss.

**456.** KARVONEN, MATTI. Convergence in industry evolution. 2011. Diss.

**457.** KINNUNEN, TEEMU .Bag-of-features approach to unsupervised visual object categorisation. 2011. Diss.

**458.** RUUSKANEN, VESA. Design aspects of megawatt-range direct-driven permanent magnet wind generators. 2011. Diss.

**459.** WINTER, SUSANNA. Network effects: scale development and implications for new product performance. 2011. Diss.

**460.** JÄÄSKELÄINEN, ANSSI. Integrating user experience into early phases of software development. 2011. Diss.

**461.** KÄÄRIÄINEN, TOMMI. Polymer surface modification by atomic layer deposition. 2011. Diss.

**462.** KOCHURA, ALEKSEY. Growth, magnetic and transport properties of InSb and II-IV-As2 semiconductors doped with manganese. 2011. Diss.

**463.** PUTKIRANTA, ANTERO. Possibilities and challenges of longitudinal studies in operations management. 2011. Diss.

**464.** HAPPONEN, ARI. Muuttuvaan kysyntään sopeutuva varastonohjausmalli. 2011. Diss.

**465.** VASAVA, PARITOSH. Application of computational fluid dynamics in modelling blood flow in human thoracic aorta. 2011. Diss.

**466.** PURO, LIISA. Identification of extractives and polysaccharides as foulants in membrane filtration of pulp and paper mill effluents. 2011. Diss.

**467.** LAPPALAINEN, PIA. Socially Competent Leadership – predictors, impacts and skilling in engineering. 2012. Diss.

**468.** PLAMTHOTTATHIL, ANSHY OONNITTAN. Application of electrokinetic Fenton process for the remediation of soil contaminated with HCB. 2012. Diss.

**469.** EBRAHIMI, FATEMEH. Synthesis of percarboxylic acids in microreactor. 2012. Diss.

**470.** JANTUNEN, SAMI. Making sense of software product requirements. 2012. Diss.

**471.** VILKO, JYRI. Approaches to supply chain risk management: identification, analysis and control. 2012. Diss.

**472.** TANSKANEN, VESA. CDF modelling of direct contact condensation in suppression pools by applying condensation models of separated flow. 2012. Diss.

**473.** HUHTANEN MIKKO. Software for design of experiments and response modelling of cake filtration applications. 2012. Diss.

**474.** PARJANEN, SATU. Creating possibilities for collective creativity
Brokerage functions in practice-based innovation. 2012. Diss.

**475.** KUKKONEN, SAKU. Generalized differential evolution for global multi-objective optimization with constraints. 2012. Diss.

**476.** LAAKSONEN, JONNA. Tactile-proprioceptive robotic grasping. 2012. Diss.

**477.** KALLIO, ANNE. Enhancing absorptive capacity in a non-research and development context
An action research approach to converting individual observations into organizational awareness. 2012. Diss.

**478.** LÄTTILÄ, LAURI. Improving transportation and warehousing efficiency with simulation based decision support systems. 2012. Diss.