Technology Strategy Board
Driving Innovation

Ensuring trust in digital services

PROJECT DIRECTORY

Introduction

Establishing trust and confidence when doing business and carrying out personal transactions is a major challenge in the world of digital services.

That is why the Technology Strategy Board, together with the Research Councils, is investing more than £14m in innovative research and development projects in this area. The projects will help to accelerate the introduction of more secure and trustworthy information systems and ensure that the privacy and consent of individuals is maintained.

The funded projects will develop trusted and trustworthy tools, technologies and methodologies to combat the risks that consumers, businesses and public sector organisations increasingly face during online transactions. The investment will also help to create competitive advantage for UK businesses by building strong capability in this country and to make home-grown businesses more globally competitive.

Thirteen major collaborative research projects, each lasting up to three years and involving a total of 52 UK companies, universities and other organisations, will share £12.84m; 19 shorter projects, each led by an SME or micro-company and lasting up to one year, will receive investment of £1.25 million between them.

This booklet highlights the activities of many of those projects, all seeking to make our digital transactions more secure and trusted.

Abies Ltd

Revocable patient consent management technology for enhancing patient trust in health information services (miCONSENT)

14 Pinewood Crescent
Hermitage
Thatcham
Berkshire
RG18 9WL

Tim Benson
E tim.benson@abies.co.uk
T (01635) 203162
W www.abies.co.uk
@timbenson

Partner: Cardiff University

What was the business need that motivated the project?

Patients cannot currently take an active role in formulating the consent policies that define who can access what aspects of their information and for how long. They cannot give and revoke consent as and when they wish, nor withdraw their consent later. Such lack of control by the data subject engenders distrust of distributed information services, which are otherwise beneficial.

What approach did you take to address the challenge?

Our project complements existing privacy-enabling technologies by creating a revocable consent management service; this supports information sharing through the 'patient journey' with whomever the patient wishes to share their records. Our project is based on recent research on how best to share information beyond the perimeters of a secure information governance network.

Our technology links the patient, their information and its access control policy. This is de-perimeterised access control.

What are the potential benefits?

Using a patient-centric consent management portal, patients can control access to their information, approve or deny requests – subject to overrides for emergency situations – change their minds and revoke consent at a later date. This development effectively puts the patient in control of their information. The patient becomes the data controller for use outside the originating organisation's secure perimeter.

What are the next steps?

Our project will define a standard to be submitted to at least one international standards development organisation dealing with health security and interoperability. We will also demonstrate an implementation of the proposed standard.

AIMES Grid Services

Shared services health applications and resources environment project (SHARE)

Liverpool Innovation Park
2nd Floor, Baird House
Edge Lane
Liverpool
Merseyside L7 9NJ

Dennis Kehoe
E dennis.kehoe@aimes.net
T (0151) 905 9701
W www.AIMESgridservices.com

Partner: Institute of Child Health

What was the business need that motivated the project?

The SHARE project addresses the challenge of providing secure access to health data. Increasing demands on services have highlighted the need for improved understanding of public health. Issues of trust and security have so far limited the application of a 'cloud' model to the storage and processing of data, preventing the UK's health research community from exploiting 'cloud' infrastructure.

What approach did you take to address the challenge?

Our project created a technology demonstrator with a shared services architecture ensuring health data used was resilient, secure and accessible, employing a 'cloud' environment. We addressed three areas associated with ensuring that third party provisioning of data is a trusted service: it conforms to a service level agreement; the service provides authentication; and, lastly, it complies with existing data security ISO27001 and N3.

What are the potential benefits?

We will demonstrate how 'cloud' services can benefit UK health research within the area of paediatric epidemiology. Our project provides a secure infrastructure within the AIMES data centre in Liverpool, allowing health informatics workers access to third party information on a commercial basis. The project is expected to lead to creation of two new posts and the safeguarding of two existing jobs. For end-users, we anticipate annual savings of £250k.

What are the next steps?

The UK is well placed to develop research capability and deliver third party services in this area through the provision of effective epidemiological record-linkage and analytic services. A commercial deployment of the SHARE infrastructure has now been established at the AIMES enterprise-class data centre.

Avoco Secure

CloudTrust

16 St. Martin's-le-Grand
London
EC1A 4EE

Susan Morrow
E susan.morrow@avocosecure.com
T 07917 507826
W www.avocosecure.com
@susiemorrow

Partners: Private Planet Ltd, Telefonica O2 Europe PLC, Imperial College London

What was the business need that motivated the project?

There has been a dramatic increase in the use of the internet by consumers. This is believed to be caused by the explosion of the social networking platforms. The number of adults using the internet has doubled since 2006, 31% of them through mobile phones. CloudTrust is perfectly timed to service this increased consumer use of the internet.

What approach did you take to address the challenge?

The consortium members have created a model based on storing users' content within a 'cloud' environment, accessible across both mobile and traditional computing platforms. Integration with the latest consumer identity technology adds the dimensions of privacy, security and user centricity demanded by today's experienced internet users. The solution is based on a number of integration points that offer users secure access and protected sharing of resources.

What are the potential benefits?

The project will benefit consortium member companies by creating a valuable solution, saleable within a global marketplace. The digital identity marketplace is worth up to US$12bn according to analysts Forrester; estimates for 'cloud' computing are US$42bn (International Data Corporation). The solution will bring to market the first user-centric and secure platform for hosting and sharing consumer content.

What are the next steps?

The consortium companies are currently working on the identified integration points and bringing the solution together to form a demonstrable offering. We are also working to disseminate the ideas around the solution. The product can be commercialised as a consumer content-hosting platform.

Cambrensis Ltd

Toward a global standard for secure and trusted exchange of digital information on systems risk

Ruxton House
Kings Caple
Herefordshire
HR1 4TX

Richard Byford
E richard.byford@intradependency.com
T 0871 218 0880
W www.intradependency.com

Partners: Intradependency Ltd, The Open Group

What was the business need that motivated the project?

We wanted to enable the exchange of interdependency data between organisations, to assure resilience of the national infrastructure and to actively manage risk.

What approach did you take to address the challenge?

Our development partner, Intradependency, is developing the process of dependency modelling to full maturity so that organisations can exchange information on which they depend and thereby improve resilience and continuity of service. The interchange of data is being expressed in vendor-neutral terms so that it can be published as an Open Standard. The Open Group has committed to publishing the standard during 2012 and is assisting in its preparation.

What are the potential benefits?

Users of the standard will be able to publish and receive data regarding the status of things on which they depend. The data will enable them to understand and monitor factors which will affect their ability to achieve their objectives.

What are the next steps?

The standard will be published in Spring 2012. If you would like information on progress please contact The Open Group via i.dobson@opengroup.org. For details of the modelling tool, iDepend®, contact Intradependency Ltd via enquiries@intradependency.com.

Chronos Technology

SENTINEL

Stowfield House
Upper Stowfield
Lydbrook
Gloucestershire
GL17 9PD

Louise Davies
E louise.davies@chronos.co.uk
T (01594) 862227
W www.chronos.co.uk

Partners: Association of Chief Police Officers, General Lighthouse Authorities, Ordnance Survey, National Physical Laboratory Timing Metrology Division, University of Bath Electronic & Electrical Engineering Faculty, Thatcham Security

What was the business need that motivated the project?

Our SENTINEL project will research and develop a service to establish the extent to which global navigation satellite systems (GPS and Galileo) and/or eLoran positioning, navigation and timing signals can be trusted by users on a 24x7 basis.

What approach did you take to address the challenge?

We are actively researching a technique to locate, quantify and detect interference with global navigation satellite systems and its consequent impact on critical national infrastructure.

What are the potential benefits?

A trusted service will enable greater resiliency and robustness of position navigation and timing systems.

What are the next steps?

Commercialisation will be achieved through partnerships, technological developments and understanding market requirements. Further private investment will capitalise on this research commercially.

Constellation Technologies Ltd

Trusted test bed prototype for biotech sector to use 'cloud' computing in large scale gene analysis

Rutherford Appleton Laboratory
Harwell Innovation Campus
Didcot
Oxon
OX11 0QX

Nick Trigg
E nick.trigg@constellationtechnologies.com
T (01235) 778275
W www.constellationtechnologies.com

Partners: AnurOS Ltd, Active Web Solutions Ltd

What was the business need that motivated the project?

Constellation Technologies is developing a solution to the next big problem in life science research. We are applying our expertise in large data and world-leading knowledge of data security to the challenge of using human genome information to develop the next generation of targeted drugs and therapies, sometimes called 'personalised medicine'.

What approach did you take to address the challenge?

We combined the latest technologies developed in the particle physics academic domain – for example, very large data sets, high security and 'cloud' computing – with the latest applications and tools in the bioinformatics sector. The result is a highly secure, easy-to-use software product for any life science company interested in genomics, proteomics and the management of clinical data.

What are the potential benefits?

The potential benefits are huge. The excitement around sequencing the genome and using the data to develop new target drugs is immense. However, the challenges lie in the enormous data sets and the very high security required by the industry and regulators. Addressing these problems will allow the life science industry to take advantage of this exciting branch of science for the benefit of everyone's health.

What are the next steps?

We are already promoting the system developed so far, adding functionality to the product and joining forces with the UK and other European academic facilities to provide a service to bioinformaticians. The industry is showing great interest.

Consult Hyperion

Sure Identity

Tweed House
12 The Mount
Guildford
Surrey
GU2 4HN

Philip James
E philip.james@chyp.com
T (01483) 301793
W www.chyp.com

Partners: Visa Europe, Codes and Ciphers

What was the business need that motivated the project?

There is mistrust of new technology and an aversion to enrolment processes. Sure Identity introduces an innovative payment card, 'CodeSure', that combines a standard payment card (where the cardholder identity has been verified by a bank) with integrated keypad and display. Consumers enter a PIN into the card and are authenticated for both financial and non-payment (DirectGov) services.

What approach did you take to address the challenge?

We based development of a proof-of-concept model upon the existing Visa CodeSure product, consisting of an authentication token and web-services. We researched security and privacy issues for such a card and then carried out controlled testing of the system to show its user-acceptability in various environments. Our innovation is a trusted token that can be made easily available to consumers for digital and financial inclusion to online services.

What are the potential benefits?

Our project examined the acceptability of using a bank token as an identity token for online services. The token combines financial and government authentication in a single bank-issued card, which it was feared users might not have accepted. Our testing showed that the great majority of users are comfortable with the concept as designed and that these results satisfy a critical parameter toward further development.

What are the next steps?

Encouraged by pretty favourable responses from our research into consumer attitudes, we will continue to explore this opportunity in the light of the announcements by the Cabinet Office regarding the Identity Assurance Programme.

Distributed Management Systems Ltd

Trusted authentication at the application level

Stockclough Lane
Blackburn
Lancashire
BB2 5JR

Basil Philipsz
E basilcasque@casque.co.uk
T (01254) 208419
W www.dms-soft.com

Partners: Amor Group

What was the business need that motivated the project?

CASQUE SNR is the next generation authentication technology. The CASQUE token is used to provide multi-factor authentication at log-in, either to an operating system or a gateway. Our project investigated how this could best be applied to authentication at the application layer so that both user and host could mutually verify each other and so establish digital trust.

What approach did you take to address the challenge?

The project team defined protocols for each application interface and realised these with detailed design and code implementations. We have completed templates to implement web hosts in order to authenticate users-by-host and hosts-by-user for .net architectures and have produced functional demonstrations. A new product has now evolved called CloudCASQUE which is the only system that addresses mutual authentication user-by-host and host-by-user with the same technology.

What are the potential benefits?

Our partner, Amor, has developed a detailed marketing plan both for the CloudCASQUE product and its managed service incarnation, identifying early adopters. Many federated authentication technologies have complex protocols which are difficult for web developers to incorporate and do not include provision against phishing. CloudCASQUE delivers high assurance, federated, mutual authentication with minimal development requirements. We feel that CloudCASQUE removes the important block to 'cloud' adoption – mutual trust.

What are the next steps?

Various blue-chip organisations have already expressed interest in CloudCASQUE and the benefits it offers. We are working with these organisations and understanding how best to position CloudCASQUE within the marketplace. A full launch of CloudCASQUE is scheduled for January 2012.

First Cyber Security Ltd

Effective and usable anti-phishing and web authentication tool

Station House
Connaught Road
Brookwood
Woking
Surrey
GU24 0ER

Rod Pugh
E rod.pugh@firstcybersecurity.com
T 08450 564232
W www.firstcybersecurity.com
@rodpugh

Partners: University College London

What was the business need that motivated the project?

Fraud is rife on the internet, with consumers being defrauded by fake websites and brands damaged. Traditional anti-phishing and anti-fraud solutions are either not noticed by users or are easily spoofed by fraudsters. An anti-fraud, anti-phishing solution is needed that is not only technically effective and powerful but also demonstrably noticeable by consumers, easy to understand and use.

What approach did you take to address the challenge?

UCL first ran simulated shopping studies. Eyetracking indicated the tool was highly noticeable and guided users towards sites it rated as safe and away from sites it rated as unsafe or unknown. It aided consumers even when they were under time pressure and when there were strong financial incentives for shopping with riskier sites. Results made our tool easier to understand and it offered a faster service to protected sites.

What are the potential benefits?

The graphical user interface was reconfigured to provide more meaningful responses, removing a potentially negative interpretation of results. The service now alerts protected websites that an attack may be under way as soon as a customer using the system visits a problem page. This reduces opportunities for consumers to be defrauded and brands to be damaged. Other security functionality has been added, resulting in a more acceptable all-round solution.

What are the next steps?

We want to carry out a study at a Russell Group university to explore the technology's suitability for protecting the institution and students from fraudulent websites. The aim is to assess ease of integration, impact on support services and user satisfaction and engagement with institutional online services as well as with the wider UK 'online ecosystem'.

Hewlett Packard

Trust domains: a framework for modelling and designing e-services infrastructures for controlled sharing of information

Long Down Avenue
Stoke Gifford
Bristol
BS34 8QZ

Adrian Baldwin
E adrian.baldwin@hp.com
T 07760 623353

Partners: Perpetuity Research and Consultancy International Limited, University of Aberdeen, University of Birmingham, University of Oxford

What was the business need that motivated the project?

Over the next few years we expect the emergence of a 'cloud-based' service world providing business with new ways to collaborate and consume IT. We see a need for tools, methodologies and better infrastructure components to help ensure service providers can offer an appropriate trade-off between security and their business needs.

What approach did you take to address the challenge?

Our project builds on previous research into security analytics and trusted infrastructure, producing a combined approach in joining up risk planning and infrastructure and operations within the security management life-cycle. Within the project we will develop technologies and risk modelling for policy-controlled sharing of information, drawing trust domains around client computers, back-end infrastructure and services. We are starting the project with empirical studies to understand enterprise trust requirements.

What are the potential benefits?

There are major business opportunities for rapidly deployable cross-organisational trusted services but these rely on having the right technologies to create policy-controlled infrastructures. We see benefits for many companies in enabling the deployment of safe services allowing information sharing and collaboration. More specifically, we see markets for services around the design, deployment and operation of trusted services as well as the potential for software products in this area.

What are the next steps?

Our project is in its early stages. We are developing conceptual frameworks and taxonomies for specifying, modelling and analysing trusted infrastructures and the information flows that they will control. This forms the basis for the future infrastructure developments as well as tools and methodologies for their deployment.

Hewlett-Packard Labs

EnCoRe – ensuring consent and revocation

Long Down Avenue
Stoke Gifford
Bristol
BS34 8QZ

Marco Casassa Mont
E mcm@hplb.hpl.hp.com
T (0117) 3128794
W www.encore-project.info
@encore_project

Partners: HW Communications, London School of Economics and Political Science, University of Oxford, Qinetiq

What was the business need that motivated the project?

The lack of flexible and intuitive controls – including the specification and enforcement of data subjects' consent – over the use and sharing of personal data is limiting the adoption of web, government and 'cloud' services by citizens and consumers.
To address this need, EnCoRe provides user-friendly, reliable, privacy management capabilities in the form of dynamic consent.

What approach did you take to address the challenge?

Although notions of consent are given much lip service, all too often consent is presented as a one-time, 'take it or leave it' option.
The challenges faced by EnCoRe were therefore to provide reliable and enforceable privacy options that integrate across organisational boundaries and legal and legacy systems. EnCoRe's innovative solution is the provision of dynamic consent capabilities that enable data subjects easily to give and revoke their consent.

What are the potential benefits?

Issues of privacy and user control are critical for the successful adoption of commercial, government and 'cloud' services. Specifically they are critical for the adoption of the Identify Assurance (IdA) programme. EnCoRe provides viable solutions to ensure the successful deployment of the IdA ecosystem. More generally, the dynamic consent approach has the potential to transform the ethical oversight of bio-banking as well as encouraging the wider adoption of various online services.

What are the next steps?

EnCoRe is entering its exploitation phase. We have begun discussions with various parties, nationally and internationally, on rolling out dynamic consent capabilities and associated products and services, such as regulatory oversight mechanisms and risk assessment methods. In addition, the partners are disseminating the results of the research in academic and industry publications.

InTouch Ltd

Faith – building trust between citizens, local authorities and contractors

66-67 Marine Road
Morecambe
Lancashire
LA4 4ET

John Walden
E laura@intouch-ltd.com
T (01524) 833588
W www.intouch-ltd.com

Partners: Lancaster University, Carillion Plc

What was the business need that motivated the project?

Highways maintenance is characterised by a complex set of workflows and data exchanges with significant levels of mistrust, both between the stakeholders and collectively in the data provided by the systems they use. These issues of trust are accentuated by the bid culture endemic in the industry and the remote nature of the workforces involved.

What approach did you take to address the challenge?

'Faith' will combine recent advances in pervasive computing with new trust models to deliver an innovative set of trusted digital services. These will enable more effective delivery of contracted services to local authorities and the general public. Specifically, our project will deliver a set of software services that can be used in conjunction with new and existing systems for issuing and monitoring work in order to provide evidence of trustworthiness.

What are the potential benefits?

Our project will deliver substantial benefits to businesses and public bodies, with the expectation of big savings. Increased trust in local authority services is also likely to improve their relationship with the public. Moreover, creating trust in the area of highways maintenance could generate public trust in other key council services. Another potential benefit is a reduction in carbon footprint of both councils and sub-contractors.

What are the next steps?

The project is in early stages and we have planned Innovation workshops involving several councils and major contractors. The aim of the workshop is to explore trust issues relating to people, processes and data in infrastructure maintenance. We hope to use the information gathered to speed the development of innovative trusted digital services.

MaxBox International Limited

Instant banking card issuance from a remote kiosk

11 Addison Road
Hale
Cheshire
WA15 9BQ

Graham Foster
E graham@themaxbox.com
T 07824 665905
W www.mboxi.com

Partners: CPUB Limited, KMS Kiosk Limited

What was the business need that motivated the project?

Our goal is to provide the capability for secure and instant issuing of standard bank cards from kiosks directly to the requesting customer, with no human in the loop. These kiosks, which may be placed in non-secure environments, would be considered secure because of the kiosk design and the secure communication objectives of this project.

What approach did you take to address the challenge?

Our challenge was in taking a major step forward from existing back office and in-branch processes to produce, in real time, an approved banking card. The system architecture is our own design and a key challenge is to create a secure end-to-end system that is not only technically approved by the relevant bank and security organisations, but is also trusted by consumers.

What are the potential benefits?

Technology Strategy Board funding has shortened our development timeline. We will have created a new trusted service to instantly deliver bank cards outside a bank branch, totally developed and owned by UK companies. A pilot has been agreed with Oberthur Technologies and activity will increase as roll-out begins with paying customers. We envisage further product development that will create work in the UK for both software and kiosk hardware evolution.

What are the next steps?

The scope of work will escalate following successful demonstration, leading to an expanded team and wealth creation for other UK participant companies as we move into the production phase. Future stages of this project are funded from orders by our industrial partners with their proven and established channels to market.

Microsoft Ltd

Scaleable and open framework for human and digital trust between informal and formal infrastructures in personal health care

Microsoft Campus
Thames Valley Park
Reading
Berkshire
RG6 1WG

Paul Thomas
E p.thomas@microsoft.com
T 07764 359738
W www.microsoft.com/uk

Partners: Health over Internet (HoIP), Edinburgh Napier University

What was the business need that motivated the project?

The internet is now the obvious way to carry out customer-centric business but the public sector has been denied the benefits. That is in part due to a lack of trust in identity, security and privacy technologies and infrastructures in the 'cloud'. Many services remain behind firewalls – especially in the health domain.

What approach did you take to address the challenge?

One of our main challenges was to find a way of engendering on the internet the levels of trust that we find in human interactions. Using a scenario focused on an informal care network, we modelled a Trust Framework based on commercial identity providers (Facebook, LiveID) together with high-assurance identities authenticated by banks and employers (NHS) in order to demonstrate how personal health records could be safely shared.

What are the potential benefits?

If we can establish the use of commercial identity providers and commodity-based privacy technologies for access to public services such as health, then there is the potential for reaping the same benefits as industry in terms of citizen-centric, personalised services and associated service innovation. This could usher in new models of care focusing on support for the individual in managing their own health and the health of those for whom they care.

What are the next steps?

The next stage of our programme will focus on use of the 'cloud' for policy-based access to statutory health records. Building on identity, security and privacy services from the first phase, we will augment commercial identity providers with two-factor authentication using mobile phones.

National Physical Laboratory

Test bed demonstrator to build trust in future cryptography systems

Hampton Road
Teddington
Middlesex
TW11 0LW

David Hindley
E david.hindley@npl.co.uk
T (0208) 943 6325
W www.npl.co.uk

Partners: Toshiba Research Europe Limited

What was the business need that motivated the project?

Industry, government and the individual rely heavily on digital data transfer; the protection of that data in transmission and storage is therefore vital. Current encryption systems can be rendered absolutely secure and future-proof with quantum key distribution (QKD); however potential end-users, such as the UK financial industry, require certification before investing in such technology

What approach did you take to address the challenge?

The National Physical Laboratory (NPL) and Toshiba Research Europe Limited (TREL) will deliver an objective and impartial test bed for manufacturers, system providers and customers, to test the claims of suppliers into this market. The test bed will characterise the performance and uncertainty contributions of different components in the system. We will carry out a high-profile demonstration of the system to encourage market take-up of the technology.

What are the potential benefits?

QKD will help guarantee the security of confidential digital information in commercial, government and personal transactions. It will tackle global cyber crime, help protect our economy and in doing so promote the uptake of e-services and e-government. QKD will encourage and accelerate the use of network communications and services, reducing our dependence on travel and paper-based communications. It will thus have a strong positive environmental impact.

What are the next steps?

Our exploitation plan is in three stages. Firstly, we will undertake technical development of the test bed and engage with end-users. Next will come business and service development in the initial market by partners of NPL's innovation centre. Thirdly, we will franchise out measurement services to new UK partners in the rapidly expanding market.

OnMyMobile

VRM Mail

18 St John's Innovation Centre
Cowley Road
Cambridge
CB4 0WS

Chris Bale
E cbale@onmymobile.com
T (01480) 466786
W www.onmymobile.com

Partners: Red Morning

What was the business need that motivated the project?

We identified a need for a simple, reliable and secure method of creating a 'follow-up' link between commercial activities and users of mobile/wireless devices. Many people are reluctant to hand out email addresses or phone numbers, particularly to unknown or untrusted counterparties, because of spam or phishing risks. Even if acceptable, such exchanges are too cumbersome in a public roaming environment.

What approach did you take to address the challenge?

We addressed three main issues. How do individuals give permission to websites to email them, without risking their personal email addresses? How do we give businesses a cost-effective way of securing customers' email addresses while monitoring and detecting potential breaches of customer data and transparently recovering from data breaches if they do occur? And how do we make it easier than typing an email address?

What are the potential benefits?

We believe that a key benefit our service can offer is to eliminate the need for trust between a customer and an online business at the start of the relationship. We want to give businesses and customers the ability to build trust, not to demand it immediately or require them to hand over private data too early in the customer relationship.

What are the next steps?

Our beta (web) product is currently live at http://leemail.me. The next step is a beta trial of our product on partners' websites – tourism, retail, hospitality on web and mobile – so that visitors and potential customers can give partners permission to email them, without disclosing personal email addresses.

Oxford University

Privacy value networks

Oxford Internet Institute
1 St Giles
Oxford
OX1 3JS

Ian Brown
E ian.brown@oii.ox.ac.uk
T (01865) 287213
W www.oii.ox.ac.uk/people/brown/

Partners: British Telecom, Consult Hyperion, University of Bath School of Management, University College London, University of St Andrews

What was the business need that motivated the project?

We want to generate detailed understanding of how individuals and organisations conceive privacy and identity across contexts – healthcare, financial services, education and training, social networking, broadband provision and government surveys – and time. This is to redress the current imbalance between data owners and subjects, helping privacy impact assessments to be conducted meaningfully and obtaining value for all stakeholders.

What approach did you take to address the challenge?

We deployed a range of qualitative and quantitative methods. We produced a strong empirical base for developing concepts of privacy across contexts and time frames; we investigated ways of establishing an equitable relationship between stakeholders in terms of the value and costs inherent in the collection, processing and use of personal data; we developed and applied new, validated, ethical and privacy-sensitive methodologies for the study of privacy.

What are the potential benefits?

They will include better data quality for government and business, along with increased trust and customer satisfaction. They will be better able to detect privacy concerns in customers' discourse and to understand the type of privacy problem. There will be better default settings in privacy configurations and improved customer retention.

What are the next steps?

We will make available on the internet a high-level design for a privacy-enhanced financial management smartphone app. We will incorporate privacy dictionaries and rules into a widely used linguistic analysis tool to support automated privacy discourse detection. We will also support the Identity Assurance program with further empirical studies and will publish our research outputs.

PIB-d Ltd

Personal information brokerage – feasibility study

22 Clifton Road
Newbury
Berkshire
RG14 7JT

John Harrison
E john.harrison@pib-d.net
T 07801 231693
W www.pib-d.net

Partners: University of Hertfordshire

What was the business need that motivated the project?

Individuals cannot yet use electronic networks to transfer personal information – qualifications, core identity, prescriptions and licences, for example – from one organisation to another in a trustworthy manner, confident that the information remains as issued by the originator. The barriers are part technical but result primarily from the lack of appropriate organisational and business models.

What approach did you take to address the challenge?

Individuals would be able to commission a 'broker' from a managed market and then use a broker account, firstly to register, sign-on, and communicate with multiple counterparties – both organisations (initially universities), and other individuals (initially other students). The next step would be to give permission for the transfer of personal information between counterparties. Our company, PIB-d, is a joint venture between the UK's Higher Education sector and the private sector.

What are the potential benefits?

PIB aims to create general-purpose trusted infrastructure in which individuals would enjoy enhanced convenience, privacy, and autonomy without incurring any costs. Organisations could improve the reliability and currency of customer data and be able to provide targeted marketing information to those who had shown interest. All this could be achieved without compromising privacy. The joint venture with the HE sector offers a credible route to critical mass.

What are the next steps?

Our priorities are, firstly, to complete a scoping study for a PIB pilot; and secondly to obtain sufficient funding and support to make the pilot feasible. Progress against the latter would be easier if the Cabinet Office allowed the major government departments greater freedom to explore other approaches to the creation of trusted infrastructure, alongside its own 'Identity Assurance' scheme.

Royal Holloway, University of London

Visualisation and other methods of expression (VOME)

Egham Hill
Egham
Surrey
TW20 0EX

Lizzie Coles-Kemp
E Lizzie.Coles-Kemp@rhul.ac.uk
T (01784) 443084
W www.vome.org.uk
@vome_project

Partners: Cranfield University, University of Salford, Consult Hyperion, Sunderland City Council

What was the business need that motivated the project?

The purpose of VOME is to explore how user communities engage with concepts of information privacy and consent in on-line interactions. Our aim is to develop alternative conceptual models of on-line privacy which allow users to make clearer on-line disclosure choices. These decision-making models will enable better dialogue between the designers of privacy and consent functionality and customers.

What approach did you take to address the challenge?

We adopted a truly multi-disciplinary approach, including sociology, psychology, political science, and computer science. Building upon qualitative fieldwork and analysis of existing communication methods in information security and e-safety, we produced a wide range of innovative interventions and research methods. These included participatory video, artists' workshops, a card game, online privacy dialogue frameworks and prototypes, as well as techniques for mapping information flows online.

What are the potential benefits?

Our project offers benefits to on-line service providers, manufacturers of technology used to deploy on-line services and also the general public. There has been considerable interest in this project from each of these communities.

What are the next steps?

We are currently finalising frameworks and models, at the same time as studying the dissemination and use of some of its interventions.

Swanmesh Networks Ltd

A secure and trusted community wireless mesh network (AST-Net)

24 Vincent Street
Swansea
West Glamorgan
SA1 3TY

Henry Wang
E info@swanmesh.com
T 07738 441528
W www.swanmesh.com

Partners: Premier Property

What was the business need that motivated the project?

The current community wireless mesh network is not secure. This hinders the application of this kind of network in security sensitive environments, such as healthcare, police and military sectors. Based on successfully developed congestion controlled wireless mesh networks, we sought to develop a secure routing protocol to ensure secure networking and intrusion detection and tolerance.

What approach did you take to address the challenge?

Our project developed a secure routing protocol using the following approaches to ensure the security of the wireless mesh network. Firstly, we used digital signatures to authenticate non-mutable contents in routing message and hash chains to protect mutable information. Secondly, the reputation of each node is calculated to exclude the intruded mesh node out of communications. These two approaches and the key distribution method were developed and implemented in the test bed.

What are the potential benefits?

The security feature of the wireless mesh network is attractive to users in security sensitive environments. This has attracted attention from several technical developers who provide communications infrastructure to military applications and they are currently evaluating our software. This will broaden the company's market from traditional community broadband access to more versatile secure applications, such as military and healthcare.

What are the next steps?

We want to improve the reliability of the software by debugging; also to build a stand-alone package to sell the software. We will introduce the software into an existing wireless mesh network platform to sell the secure mesh nodes and we will prepare marketing materials for the new products.

Thales Research & Technology (UK) Ltd

TEASE – trust enabling augmented reality support for information environments

Worton Drive
Reading
Berkshire
RG2 0SB

Glyn Jones
E glyn.jones@uk.thalesgroup.com
T (0118) 923 8427
W www.thalesgroup.com

Partners: Oxford University, Warwick University, HW Communications Ltd

What was the business need that motivated the project?

In our dealings with people in the real world we use our experience to judge how much trust we should place in them. In the online world we often have no way of knowing who or what we are communicating with and therefore no means of assessing how much we should trust them or what they say.

What approach did you take to address the challenge?

We provide users with a measure of the confidence they could have in online information or its source, based on the provenance of the information/source. By investigating the best way to present the measures, we can devise informative interfaces. A data processing and visualisation architecture will allow users to combine provenance data with the outputs from other trust-enabling technologies, thus enhancing their ability to determine trustworthiness.

What are the potential benefits?

Initially, tangible benefits may be apparent only to users such as government and emergency services personnel and certain businesses, needing to gather data rapidly from unknown sources. As the tools mature and become more widely used, the benefit of using high-quality information will become more obvious. The tools will then be used in a less formal context, where smartphones and tablet PCs are becoming platforms of choice.

What are the next steps?

We are approaching the mid-point of the TEASE project and are developing proof-of-concept prototypes for use in customer engagement by our industrial partners. Thales is focusing on the potential for trustworthiness service offerings while HW Communications is interested in applications at the consumer end of the market.

The VoxGen Group

Enhancing voice biometrics

Centre Point Tower
101-103 New Oxford Street
London
WC1A 1DD

John Salter
E jsalter@voxgen.com
T (0207) 4205900
W www.voxgen.com

Partner: Mydex

What was the business need that motivated the project?

In spite of achieving remarkable results in the laboratory, voice biometrics are virtually unused in Britain. Yet the urgent need for improved security around personal data has forced businesses to impose increasingly onerous knowledge-based security checks that are notoriously ineffective in preventing fraud while simultaneously inconveniencing customers and alienating them from automatic systems.

What approach did you take to address the challenge?

VoxGen and our partner, Mydex, are working to enhance the traditional approach to voice biometrics by adding a second factor to the verification process – personal knowledge. This requires us to develop a statistically rigorous probabilistic reasoning system to combine these two incongruent data points. No-one has actually tested this concept properly until now. Our success would lead to higher security, greater robustness of application and an easier-to-use customer experience.

What are the potential benefits?

The primary benefits are social and economic. The online consumer is subjected to an intolerable threat of theft from organised crime across the world. Keeping up with the evolving nature of this threat drains a growing amount of society's resources. Getting a usable and secure multi-factor biometric system in place, one that is easily but securely updated, will dramatically ease the burden of monitoring such criminal activity.

What are the next steps?

We intend to create products using technology developed by VoxGen to give ordinary consumers the power to control their personal online data. Our work will enable them to add additional security measures and to open up the voice channel to online data.

Voicekey Limited

Personal identity management using voice biometrics

Centre of Innovation & Technology Exploitation
Nottingham Trent University
Clifton Campus
Nottingham
NG11 8NS

John Weightman
E john.weightman@voicekey.co.uk
T 07554 539792
W www.voicekey.co.uk

Partners: Mason Infotech Ltd

What was the business need that motivated the project?

The impetus for our project came from the need to provide a secure identity management service, capable of establishing trustworthy access to remote information systems. Verifying the identity of an individual accessing a remote service is difficult. Our voice biometric solution confirms an individual's right of use in a simple and straightforward manner.

What approach did you take to address the challenge?

The technical approach we adopted was to develop a system demonstrator, based on our patented voice biometric technology. The fast-track project developed the VoicekeyID donor technology for use on mobile and call centre platforms. VoicekeyID is innovative in that it allows users to store their encoded voice biometric classifier (Voicekey) on their mobile platforms and use them in trusted peer-to-peer interactions with variety of different organisations.

What are the potential benefits?

Our project has been very successful and we have demonstrated the developed solution to a spectrum of high profile players, generating considerable market interest. The team is driving market exploitation and we believe that they will be of significant economic and social benefit to the UK. Without the award of the Fast Track Trusted Services project this work would not have taken place in the current timescales.

What are the next steps?

We have used the project and system demonstrator to strengthen our current business plan. This will be used to secure additional funding which will finance the commercialisation of our technology. Discussions are ongoing with a variety of industrial players to develop commercial partnerships and revenue streams.

Whatever Software Contracts Limited

Cleanband

Castlewood House
77-91 New Oxford Street
London
WC1A 1DG

Grant Kaufmann
E gkaufmann@cleanband.com
T (0203) 4116659
W www.cleanband.com

Partner: RedPixie Limited

What was the business need that motivated the project?

The cost of poor internet security is high. This can be seen in internet banking being compromised, personal data being stolen or destroyed or a child being traumatised after being bullied or visiting an undesirable website. In order to protect oneself online, however, it should not be necessary to become a computer security expert.

What approach did you take to address the challenge?

Internet safety solutions currently require extensive technical skill, are extremely inflexible or easy to bypass. Cleanband solves this by introducing a Trusted Authority that subscribers can select themselves. This could be an NGO, a school or a religious organisation that the subscriber trusts to make a recommendation about what should be accessible on the internet. Full customisation is also possible, leading to a flexible and safe internet service at home.

What are the potential benefits?

Cleanband will allow parents who are less technically skilled than their children to have confidence that their home internet connection is protected. This will minimise internet crime, reduce the incidence of online bullying and restrict the viewing of harmful material. The result is that parents can allow their children to explore the internet and develop critical skills without fear of them accessing unacceptable content or visiting undesirable chat rooms.

What are the next steps?

We are currently in discussion with an internet service provider (ISP) partner who is interested in implementing Cleanband in the UK. They are running an initial trial and a full release is expected in the next few months. The next stage will be to target interested ISPs in Europe.

Technology Strategy Board

Driving Innovation

The Technology Strategy Board is a business-led executive non-departmental public body, established by the Government. Its role is to promote and support research into, and development and exploitation of, technology and innovation for the benefit of UK business, in order to increase economic growth and improve quality of life.

Disclaimer

The entries in this directory were provided by the individual companies. The Technology Strategy Board cannot guarantee the accuracy or completeness of any of the information.

Technology Strategy Board
North Star House
North Star Avenue
Swindon
SN2 1UE

Telephone: 01793 442700

www.innovateuk.org