Technology Strategy Board
Driving Innovation

Results of competition: SBRI - Preventing fraud in M-Commerce - Phase 2

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
AlphaFox Systems Limited	Crystal Key - An Unforgeable Unclonable Personal Verification System	£99,960	£99,960

Project description (provided by applicants)

Crystal Key - An Unforgeable Unclonable Personal Verification System:

The core of the AlphaFox Systems Ltd project is the further development and launch of a Personal Verification System for mobile phone transactions ('m-commerce'). It is based on an unclonable (i.e. non-forgeable) and unique physical optical 'personal identification tag', called Crystal Key™, that the consumer carries with them locked within a small device on their key-ring, purse, wallet, or similar personal item. The device is the size of a lipstick or key-ring micro-torch and comprises a tag with a randomly-distributed array of 'crystals' in it with integrated light source. When verifying personal identity while making an m-commerce transaction, etc., the mobile phone (or tablet) application ('pictorially') asks the consumer to hold the Crystal Key™ device up to the phone camera which automatically takes a photograph of the tag within the device and compares the image of the tag's random 3D crystal array/pattern with that stored on the payment verification database for that consumer. If there is not a match between the two images, then the transaction will be denied. Hence only legitimate transactions can occur.

The Internet and, increasingly, (mobile phone) m-commerce are becoming the driving force behind commerce and retailing, allowing even the smallest and newest of companies to trade internationally. Similarly, an increasing number of consumers carry out transactions on sites that they are not familiar with. This is providing additional opportunities to fraudsters to exploit loopholes in the security and authentication of transactions, identity fraud, etc.: e.g. Is the payment site genuine? Is the payer who they say they are?, etc. It is now essential that transaction systems are able to verify the authenticity of the purchaser and the identity/legitimacy of the vendor.

Modern RFID chips could provide the basis of the tag, but most mobile phones do not contain RFID readers. What is required is a system that exploits a mobile device's current range of sensor technologies, i.e. the camera. AlphaFox uses randomly produced 'photographable' optical features ('tags') that are unique to each user and that cannot be copied. Anyone attempting to copy the 3D features will fail due to the vast

number of mathematical variants that are possible (billions). It has already been demonstrated that fingerprint and facial recognition can be spoofed, due to their essentially 2D nature (i.e. photographs can be used to spoof them).

AlphaFox's Phase 2 project builds on the success of Phase 1, taking it from proof of principle to market launch, and will meet all of the above needs by providing a 'tag' locked within a device that is unique to each individual consumer and which can be read using any smart phone, tablet, or webcam camera – and across all mobile platforms. It will be inclusive in that those with a wide range of IT competence including technophobes will be able to use it, as will people of limited dexterity and sightedness, and people from different cultures, since this simple verification step does not involve reading, typing, speaking, remembering, PINs, or use of bank cards. It will empower m-commerce.

Technology Strategy Board
Driving Innovation

Results of competition: SBRI - Preventing fraud in M-Commerce - Phase 2

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
HoiP Telecom Ltd	IProve - Authentication as a Service	£98,800	£98,800

Project description (provided by applicants)

IProve - Authentication as a Service

The hardware and software authentication devices market is witnessing increasing growth in revenues (US$ 760 million by 2014). Companies integrating mobile OTP (One Time Password), OTP tokens and USB tokens into their networks decrease the risks of data breach and improve their overall security stance. As the authentication market evolves, organizations will look at purchasing advanced security technology that will protect their data and that of their clients by requiring a user to have multiple factors of identification before gaining access to a workstation or network device. This significantly reduces the possibility of theft and prevents the compromise of an entire system due to a compromised password.

Delivering instant remote access is no longer just about remote employees. It's about enabling customers to perform online transactions, mobile sales personnel to access ERP (Enterprise Resource Planning) applications, outsourced call centres to share the customer database, and more. While ensuring reliable, instantaneous access is a must, so, too, is the need to guard against breaches and ensure continuous governance. In this business environment, strong authentication—using multiple factors to ensure users are indeed who they claim to be—is increasingly essential to reduce fraud. As they evaluate the alternatives, many organizations are opting to use SMS based authentication, which offers a mix of convenience and security that make it ideally suited to many usage scenarios.

IProve combines the security of two-factor authentication with the convenience and simplicity of mobile devices and SMS messages. IProve can present a number of significant benefits:

- Improved security. IProve delivers two-factor authentication that offers a number of security advantages over basic username and password access, helping provide a strong layer of protection for user access and identities.

- Reduced security costs. Compared to hardware-based token approaches, IProve can provide both significant upfront savings—by reducing token purchases and distribution costs—and over the long term by streamlining administration and eliminating the cost of replacing lost tokens.
- Boost deployment opportunities. By eliminating tokens from the equation and relying instead on ubiquitous mobile devices, IProve brings two-factor authentication to a range of arenas where it would have been previously impractical—online banking, controlled access to valuable IP, e-learning education portals, authenticating voice-based system access, healthcare sites.

IProve offers numerous advantages and benefits. In addition, its lower costs and ubiquity make it an ideal complement to an organization's existing security and authentication mechanisms. For many organizations, IProve can present a host of benefits to organizations looking to improve security while maximizing the productivity of end users and administrative staff.

Technology Strategy Board
Driving Innovation

Results of competition: SBRI - Preventing fraud in M-Commerce - Phase 2

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Kasra Limited	MyKey: Enabling Faster & Safer Access to Mobile Services	£95,844	£95,844

Project description (provided by applicants)

Mobile phones have significantly increased in numbers and capabilities in the recent years. Communications aside, they have also become a digital portal for accessing and utilising a wide-range of services on the go. The transfer of services/apps from traditional PCs/desktops to mobile devices is accelerated by increased service accessibility and user convenience. The mobile feature of these devices has also inspired a whole range of new apps/services e.g. location-based searches, navigation apps, QR/bar code scanners, and mobile payments.

Although the benefits of smart phones and mobile services are clear, the associated risks (due to increased exposure and the portable nature of these devices) are relatively less publicised. Pins & passwords are commonly used for user authentication / access control. They are simple and intuitive but admittedly not so easy to use and apply effectively (i.e. there lies much inconvenience in setting and managing strong passwords). Multi-factor authentication protocols aim to improve on this with an added layer of protection – often relying on an additional item to be carried (e.g. a security token) or presentation of a personal feature such as a facial scan, fingerprint, or vocal reading. There is increasing discomfort in the use of such second level authentication protocols; mainly due to their additional physical effort and/or privacy implications.

MyKey is a new second-layer authentication service, for mobile devices, that is physically and memory-wise effortless – this means you do not need to memorise any phrases, carry any additional devices, or indeed perform any extraneous actions such as swiping your finger, reading sentences, or scanning your face. MyKey uses behavioural signatures to authenticate access and protects user privacy by scrambling sensitive data on user device (before transmission to the server). When a trusted user interacts with the device, MyKey can detect this and grants access. When an unknown party accesses the device, MyKey detects the change in behaviour, locks the device and enforces additional security checks to ensure authorised access.

MyKey helps users to adopt and use mobile services in a safe, secure, and convenient manner, while at the same time imposing tight security checks and controls on the unknowns and strangers who attempt to access a device or its services. MyKey accelerates business via mobile technology.

Results of competition: SBRI - Preventing fraud in M-Commerce - Phase 2

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
VIX Technology UK Ltd	Secure closed loop mobile ticketing for public transport	£98,756	£98,756

Project description (provided by applicants)

The objective of this phase 2 project is to develop a closed loop mobile ticketing solution for commuter public transport which has strong fraud prevention measures and provides rich data to operators and passengers. Within the public transport market the growing trend towards mobile ticketing solutions is in recognition of the reduction in capital and operational costs compared to traditional cash and smartcard based systems and the growing expectations from passengers that they should be able to pay for transport using their smart phone. With Gartner reporting that smart phone sales grew by 46.5 per cent in the second quarter of 2013 and exceeded feature phone sales for the first time the potential market for mobile ticketing continues to expand.

A full mobile ticketing solution consists of three elements. The back office server element provides account management and product sales functions. The smart phone element enables a customer to purchase and display their tickets. Finally, an on vehicle 2D barcode scanner provides automated validation and fraud prevention to protect both the transit operator and the travelling customer. The on-vehicle validator also provides data on ticket usage to the back office to enable data analysis and business intelligence functions. Most mobile ticketing solutions without an on-vehicle validator are susceptible to fraud and have reduced ticketing data available for analysis.

Above all the solution must be convenient, performant, secure and robust for both the transit operators and the travelling customer. The solution must answer the needs of both the transit operator and the travelling customer and be convenient for both. If the mobile device is lost or stolen, the customer must be able to redeem their tickets on alternative devices. Providing a solution that addresses both fraud and customer service requirements is challenging and a key objective of this project.

From the transit operators perspective a clear objective of the project is to help remove financial barriers and leverage previous capital investment by using existing equipment in new and innovative ways to enable a mobile ticketing solution for multiple ticket types. At the same time for those operators without existing infrastructure, the project seeks to provide a low cost, simple to mobile ticketing solution that requires

minimal capital investment and low running costs.

Mobile ticketing systems provide new and exciting market opportunities, but in order to understand the impact of these in an operational context is a significant challenge. Incorporating these data into the data warehouse and incorporating them into big data analyses is another objective of this project.

Results of competition: SBRI - Preventing fraud in M-Commerce - Phase 2

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
Voicekey Limited	mTrust: A low cost inclusive m-commerce solution for high street and online trusted traders	£98,983	£98,983

Project description (provided by applicants)

mTrust: A low cost inclusive m-commerce solution for high street and online trusted traders.

The purpose of this project is to design, implement and make market ready the operational software and inclusive user interface for the Voicekey mTrust mobile commerce trusted mtrader scheme.

The introduction of mcommerce products into an already crowded small value transaction processing market has many obstacles to overcome in order to attain market acceptance. Alternatives such as Chip and Pin, as well as its wireless derivative Pay-wave, are well established and many consumers will be reluctant to take up alternatives that are seen as either less secure or more complicated to process. Add to this the issues associated with the accessibility of mobile applications and it is possible that mcommerce will find it difficult to gain traction in such a mature market.

The Voicekey mTrust trusted mtrader scheme aims to address both vendor and user reluctance to mcommerce deployments as well as addressing all user accessibility issues. The hardware cost associated with our solution is very low, consisting of existing or low cost mobile retail point of sale units and consumer mobile phones. To initiate a transaction, consumers need only to activate an APP on their phone. For security purposes this APP will only activate when in the vicinity of one of the trusted mtrader units. Once activated, mutual authentication is provided by the APP being qualified to the vendor system using an identity certificate previously created from the users' voice samples during a simple registration process. This certificate is displayed to the vendor as an on-screen digital code within the APP. The vendor can thus authenticate the user using conventional bar-code point-of-sale devices. To complete the transaction, a dynamic payment certificate is wirelessly sent to the phone where it can be displayed and scanned in order to debit the cost of the transaction from the users' bank account or phone balance. A derivative of the Voicekey mTrust product can also be used to ensure remote (i.e. online) trusted transactions processing.

This will make use of secure out of band verification; developed under a previous Technology Strategy Board Smart award.

As part of the mTrust system, a carer management and user fraud prevention training aid is provided that will enable children, vulnerable and disabled users to participate in the scheme with confidence. The aid addresses financial management and fraud prevention issues such as: Security, Consequences, Limits, Permissions etc. Voicekey is working with a range of hardware suppliers to tier 1 and high street retailers. These will provide the company with access to national and global routes to market. Our collaborations with inclusive user Charities and University accessibility research groups will also ensure that the developed solution will be both trusted and accessible for all.