



Media

- › Contact the Press Office
- › Science blog
- › News releases for journalists
- › Find an expert
- › Filming in Oxford
- › For University members

17
DEC

Mobile tech 'can replace cheques'



17 Dec 09

[Technology](#)

The announcement on 16 December by the board of the UK Payments Council that cheques are to be phased out by 2018 has heightened the need for secure replacement payment systems.

New security technology developed at Oxford University by Professor Bill Roscoe and his team that allows people to make payments via mobile phones, offers a solution.



Oxford technology could mean we all pay 'by phone' in future

The technology is designed to work in almost all situations: person to person, in a shop or restaurant, at a vending machine, online, or as part of a telephone conversation.

Isis Innovation, the University of Oxford's technology transfer company, is working with Professor Roscoe to commercialise the technology.

' A key requirement of new payment systems will be the ability to make payments from person to person, such as paying a builder or a friend,' said Professor Roscoe of Oxford University's Computing Laboratory.

' What we have is technology which enables anyone to easily create a secure connection between two devices: it can work via Bluetooth, WiFi, the internet or across ordinary telephone or SMS connections.

Further information

- › Isis Innovation
- › Oxford University Computing Laboratory



' The core of our technology is a new security protocol that enables strong cryptographic keys to be created with the least possible work. The key to the protocol is that it prevents anyone from doing any searching to break into the transaction.'

The Oxford technology uses a system in which the payer checks whether a short numeric code (4-8 digits for most applications) generated within their own phone is the same as the one generated by the payee. This number is random and does not have to be kept secret. This ensures that the customer's mobile is connected to the correct store, or to the mobile of the person they wish to pay. Payment then occurs without the exchange of sensitive details such as credit card numbers or PIN.

It is expected that no hardware modifications to the phones will be needed, and the Oxford team have built demonstration systems to show a variety of uses. The payment itself could be made in a number of ways: using electronic cash or credit stored on a mobile phone, via authorisation of a credit card payment, or by instructing a bank to pay a merchant or another person a certain amount.

' The technology is designed to put the payer in charge of the connection and let him or her have direct control over how much is paid and to whom – very much like a cheque,' said Professor Roscoe.

' It is clear that banks will be looking for innovative solutions to avoid the limitations of current technology and that the ability to pay using mobile phones in the same way that you do now using a cheque will need to be phased in over the next eight years. The beauty of this system is that it can be used for many different methods of payment.'

Consider the following scenarios:

- ◆ Emma chooses a ticket online on her PC and pays with her phone. Her phone and the agency connect by telephony. She enters the code and confirms the payment, perhaps by entering her PIN.
- ◆ Jim wants to make a low-value payment, say for a bus ticket. His phone makes a Bluetooth connection with the bus, and he confirms that the codes displayed on his phone and the ticket machine are equal by buying the ticket of this choice.
- ◆ A child has run out of credit. He rings his mother, who transfers money without fuss: she has previously created a permanent key between their phones that allows her to transfer credit without the child needing to take any action.
- ◆ Jim has just finished replacing a tap for Liz. Liz pays Jim phone to phone: they simply make contact by telephone and ensure that two codes calculated by their phones agree.

In each case the comparison of the codes makes it pointless for a "man-in-the-middle" to attempt to break the payment, particularly since the payee will transfer details such as a name, logo or photograph that is then checked by the payer and included in the electronic payment instruction that automatically

goes to the bank.

The next steps are for further demonstrators of the technology to be built and for these to be taken through industry testing. Standards will need to be developed for how the protocols are to be used and how to prevent unauthorised use of the payment features on phones. Isis welcomes inquiries from commercial partners interested in being involved in further development.
