Your Bank, ID and Keys - All In One

You leave your house to go on vacation, lock the front door behind you and start the car. At the airport, you pay the parking fee and go through security with a flash of your passport before boarding your flight. On arrival, you check into your hotel and arrange for a transport pass for the exact duration of your journey before swiping on to the metro and heading to the museum you have already bought your ticket for.

A common enough scenario but what if – instead of having keys, wallet, passport and printed tickets – every single one of these interactions was performed wirelessly with your smartphone?

The established concepts of contactless payments, mobile wallets and moves towards fully mobile banking already signal a major change in the secure services that can be performed wirelessly or with a smartphone. However, leading wireless technology design and development firm Cambridge Consultants [1] says the real business value of smartphones is yet to come, with a massive disruptive effect on a much broader selection of secure services – everything from IDs and passports to website logins, anti-counterfeiting and as replacements for keys.

Jon Edgcombe, leader of the application software technologies group at Cambridge Consultants, said: “We have barely scratched the surface of what smartphones, Near Field Communication (NFC), and secure element technology can do for secure services. Mobile wallets and ticketing are just the jumping off point. The short and long-range wireless capabilities of smartphones are ripe to be exploited for a far greater range of secure applications – things like identity verification using face or voice biometrics, for example.

“We’re just at the point where the full potential of the technology for smartphones to be a central point in secure services is starting to be fulfilled. Although there are some technical challenges to overcome to get to this point, we firmly believe that smartphones will transform how consumers interact with a range of day-to-day secure items – not just your bank card and wallet but also your house and car keys, your travel tickets, loyalty schemes, healthcare devices, even corporate access and beyond.”

The smartphone has some inherent advantages that make this vision of the future possible. Not only is the device linked directly to an individual – and usually carried on their person at all times – but it offers a flexible user interface and processing platform. Moreover, increasingly the technology to secure the required connectivity, imaging or data processing capabilities is already embedded in the phone.

Jon continued: “The key limiting factor is access to the secure store of information on the device, and who controls this – the smartphone designer, the mobile network operator, a third-party ‘trusted service manager’ or the end user. The last approach – where the end user controls the secure element in the same way you currently control which apps are on your smartphone – is gaining support in some application areas. Despite this uncertainty, many

organizations – ourselves included – are looking at ways to take advantage of the technology in order to open up a whole new world of products and services in medical and pharmaceutical, home care, automotive, transport, energy and consumer markets.

“In addition, the opportunity for secure data collection, processing and communication has an immediate application in the increasingly valuable area of authentication and track and trace to secure supply chains against counterfeit or diverted products and other illegal activities, while providing an easily customizable and upgradeable set of applications and user interfaces to suit different stakeholders.”

Cambridge Consultants will be presenting seminars at two events discussing the potential business applications for smartphones helping to tackle fraud, counterfeiting and diversion of goods. The first – “Authentication and the smartphone revolution” – will take place at the 11th Asian, Middle East and African High Security Printing Conference, September 24-26 in Dubai, UAE. The second seminar – “The role of smartphones in pharmaceutical anti-counterfeit and anti-diversion protection” – will be held at the 7th Global Forum on Pharmaceutical Anti-Counterfeiting and Diversion, November 27-29 in Washington DC, USA. Both events are being organized by anti-counterfeiting analysts Reconnaissance International.

“The ubiquity of smartphones, and their technical capabilities, means the security sector has to start thinking far more intelligently about the potential applications,” said Ian Lancaster, director of Reconnaisance International. “While it may not happen overnight, the vision Cambridge Consultants has set out is certainly a compelling one. The company is one of the leading innovators in both wireless and security technology and is at the forefront of finding out just what smartphones can do for businesses and consumers. Its expertise in examining the function of smartphones in authentication and traceability will bring significant additional value to these two security events.”

For more information visit: www.CambridgeConsultants.com [1]

October 2, 2012

Source URL (retrieved on *10/26/2014 - 4:03am*):
http://www.wirelessdesignmag.com/news/2012/10/your-bank-id-and-keys-all-one?qt-digital_editions=0

Links:
[1] http://www.cambridgeconsultants.com/