CHYPpings

Spring 2008

Contents

1. Customer focus
2. Expert views
3. News and best of the blogs
4. Meet the team



Customer Focus
Commercial Bank of Qatar

There are many emerging economies investing in systems and technology that will leapfrog developed world infrastructure. A case in point is Qatar, which has developed a new man-made residential and attraction island landmass called *The Pearl*, which will operate as a cashless society.

The private island situated in Qatar's west bay will be home to over 50,000 residents and become a major attraction to a forecasted 3 million visitors annually by 2012. The developers United Development Company (UDC) in partnership with Commercialbank (Cb), Qatar's largest private bank, have formed a joint venture whose primary objective is to make The Pearl Qatar (TPQ) fully Near Field Communications (NFC) friendly by January 2009, making it the first and only NFC capable Private Island in the world.

To this end, Cb retained Consult Hyperion to help develop concepts and prototypes to demonstrate the real possibilities of new contactless and mobile technologies to the stakeholders and to help them make critical business decisions in confidence. We were then retained to develop the detailed requirement, functional and technical specifications for the systems needed to implement TPQ's NFC vision.

As you might imagine, transactional systems of this nature have safety and security aspects that are orders of magnitude more complex than for "simple" payment transactions. If you are using your mobile phone to get into your apartment, to pay at the supermarket, to exchange business cards with colleagues, to get a drink from a vending machine and even to log in to your home banking, then it has to work every time.

"By moving directly to an NFC platform, residents and visitors benefit through the convergence of personalised access control, contactless payments, loyalty and multiple e-applications that all reside on a single NFC mobile phone removing the need for bulky wallets, keys and ID cards." (Stated name title, UDC)

"TPQ represents the best in quality lifestyle and living so we wanted to embrace technologies that reflected that image so we chose NFC over simple contactless technology as it offers so much more. We envisage our residents and visitors being able to live their lives from their mobile phones as the new applications being developed and deployed with the help of experts from Consult Hyperion are truly innovative. This approach will raise the profile of both Qatar and the Gulf as a whole in the eyes of the world" commented Julian Phillips of Commercialbank.

For further information on Consult Hyperion's experience and expertise in mobile, payments and NFC prototyping and specification please contact:

Nick Norman <nick.norman@chyp.com>

Satellite image from UDC, May 2008





Phishing and signing

James Sellwood
Head of
Software Development

In the Spring 2007 issue of CHYPpings, Richard Allen explained how two-factor authentication (2FA) can be used to help increase the security of a customer logging into a banking website. The piece mentioned how more conventional passwords when used on their own are the "weak link in Internet security". Two-factor authentication helps increase the security of the authentication by allowing the bank to validate that the customer logging on, actually has access to the smart card associated with that e-banking account and also that they have the correct PIN associated with the smart card. It will not, unfortunately, end the problem of phishing but it can be part of an effective strategy to tackle the problem.

When it comes to phishing there are a number of parts to the overall attack and the security of the customer login is just part of the attack surface. Phishing, in its most common form, relies on an email being received by a customer (of any service: it's not just banking customers who are victims here) and being convincing enough that they will comply with its instructions. In most cases these phishing emails request, that the customer follow a link and then provide some amount of their service related information. You've no doubt experienced the kind of thing: 'Your account has been blocked and to activate it you must follow this link and provide security information to us before we can unblock it for you.'

Technologies such as 2FA do not actually prevent these phishing emails or make the decision about which emails are real and which are fake any easier. They also wouldn't stop customers supplying sensitive information to the phishers in most cases.

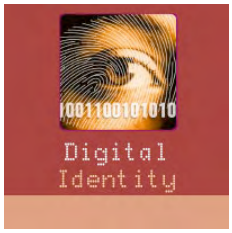
As pointed out above, the first part of a phishing attack usually involves an email and most people put a significant amount of trust, quite incorrectly, in what an email is and where it comes from. Now I don't wish to become all nostalgic for simpler times but when you used to receive a hand written letter in a hand written envelope from someone you knew, and had communicated with previously, you could normally recognise the hand writing. Even if you couldn't straight away you could always compare the recent letter to a previous one (if you had felt such a need) in order to check. In comparison the current situation with most emails is very different even though many people put as much confidence in them as they would that handwritten message. Forgery of email headers and the ability to copy not just someone's writing style but their entire message layout and imagery makes it very easy to create phishing emails which look to be from someone they are not. If only there was some way of providing the same kind of source recognition to emails that once was possible (and still is if you know people who still write them) with handwritten letters – enter stage left: digital signatures.

Email encryption has become more commonplace in recent years, with programs like PGP being used more regularly to secure sensitive business related emails. Even so, the alternative application of certificates and asymmetric cryptography, that of digitally signing an email message seems to have lagged behind. When the sender applies the private key of their key pair to 'sign' the email message before it is sent, the recipient can easily verify the sender by using the stated sender's public key. If the stated sender's public key does not correctly confirm the 'signature' then the email was not sent by someone with access to that private key and can therefore be discounted as a fake.

Once again, as always, this kind of technology does require some user training before customers will happily be able to identify when email signatures are correct or false. When the technology migrates to chip cards or, better still, mobile phones this may become much easier. Explaining how to use digital certificates in Outlook is complicated, but explaining to a customer that "if the e-mail shows up in red on your phone then the e-mail doesn't check out" is much easier.

If this can be done, then digital signatures will provide an anti-phishing defence that is much more "black and white" than anything that currently relates to phishing emails and their detection. Proving conclusively that an unsigned email is real or fake can be a difficult and highly technical job and it is one that many people get wrong at some point or other. On the other hand, checking public and private keys is something computers do easily and automatically with little chance of error. The user simply must be taught to understand the visual cues indicating the result.

For further information please contact:
James Sellwood
<james.sellwood@chyp.com>



Reputation and replicants

David Birch, Director

I went to a talk by Clay Shirky about his new book *Here Comes Everybody*. He's a very good speaker, had very cogent and thought-provoking material and has made me start reflecting on my model of identity and reputation once again. There's no point reproducing his talk since you can read the book or the blog yourselves, but there were a few points that I feel like highlighting. The core of what he said was the the technology of the Net has become boring enough to become socially interesting (in other words, my Dad reads my blog now) and one of the first-order effects of this is that media is becoming a call to action. He gave a couple of very well-chosen examples to illustrate the point (taking on the mafia in Palermo via a web site and flashmob protests in Minsk).

As Kevin Kelly observed "bottom up is never enough". At some point, there needs to be some structure in a and I think that there is some evidence to suggest that distributed reputation management may well be the only mechanism needed to achieve that once there is some genuine security in place (so that reputations cannot be hijacked). Therefore, my view of the importance of secure credentials is reinforced, because I see reputation as being the history of a virtual identity over time and that virtual identity is a collection of credentials.

One of the potentially valuable credentials that might be attached to a virtual identity might well be something along the lines of "IS_A_PERSON". Why? Well, there are plenty of situations where net discourse is subverted by the absence of such of credential.

If you have a blog where it is important that people, not bots, contribute then you might well demand to see a certificate with the IS_A_PERSON credential, even though you don't actually care which person it is. Ah, you might say, but who cares about blog posting? For important, regulated, activities such as banking then this sort of thing is irrelevant. Really? Consider the case of Las Vegas resident Adam Gregory who went on a business trip to Phoenix. He stayed at the Ritz-Carlton and charged the $1,082 bill to his American Express card, or so financial records show. In fact, Mr. Gregory didn't live in Las Vegas, never held a job and wasn't even a real person. He was a "synthetic" identity: a person who appears real on paper but is actually a fraudster's concoction designed to trick financial institutions into granting loans and issuing credit cards. There are other cases, of course, where it doesn't matter whether an identity has the IS_A_PERSON credential or not. On this blog, I don't care if a poster is a real person or a roomful of students or a bank: all I care about is that their comments add to the debate. On eBay, I don't care whether a seller is a real person or a company or whatever so long as the reputation system works properly: if you have the stars, I'll do business with you, which perhaps ought to be the web 3.0 rallying cry.

The 11th annual Consult Hyperion Digital Money Forum was held in London in April. Here are just a few of the comments we received...

"This year's Forum was fantastic, speakers were great, lively panel debates and met some good networking contacts."

"I calculate that this was my seventh Digital Money Forum and I rate it the best yet in terms of speakers, delegates and venue."

"I think it was a fabulous and well-organised event - the location was great, the food wonderful, the host relaxed and entertaining and the attendees a great mix from across the stakeholders in the industry."

"I think it was a fantastic event with some really good speakers, and made a real change to the dry sales presentations that I usually attend."

To download presentations from the Forum visit: **http://www.digitalmoneyforum.com**



We always welcome feedback. Come and visit our blogs and give us your opinions.

The Digital Money Blog
www.digitalmoneyforum.com/blog

The Digital Identity Blog
www.digitalidforum.com/blog

We also have a series of short weekly (15-20 minutes) podcasts from around the digital money and digital identity worlds that you can download from www.chyp.com/podcasts.php or from the Apple iTunes store. Just visit the iTunes podcast section and search for "Consult Hyperion" to subscribe.

Spring 2008



We are an IT consultancy that has spent two decades advising leading organisations around the world. We help them to reap real benefits from technological change in the field of secure electronic transactions: transactions ranging from retail payments to passport control and from mobile top-up to TV shopping. We help organisations to:

- ***Evaluate new business concepts*** to give clients firm foundation for new ideas.
- ***Develop new products and services*** from specification to customer roll-out
- ***Test and certify complex systems*** using structured and automated techniques.

We support customers in reaching their goals in a timely and cost-effective way. We work in:

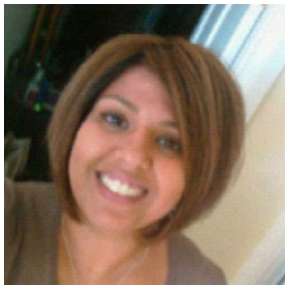
- ***Financial services*** where our clients include the world's largest payment schemes.
- ***Telecommunications and media*** where we advise world leaders such as Sky and Vodafone.
- ***Technology*** where we support some of the largest IT companies including EDS, NTT Data and Thales.
- ***Public sector*** where our work has ranged from ID card specifications to roadmaps for law enforcement.

Recognised as thought leaders in the fields of digital money and digital identity, experienced in the delivery and risk analysis of population-scale transaction systems (from identity cards to "chip and PIN" payments) we have world-class expertise at every step in the transaction value chain, ranging from the authentication of transaction using smart cards and biometrics to the execution of transactions through mobile phones, the web and digital television.

For more information about our expertise and experience or to find out how we can help you to exploit new technologies please contact:

Private Sector: Nick Norman
nick.norman@chyp.com, +44 (0)1483 468690

Public Sector: Mike Burden
mike.burden@chyp.com, +44 (0)1483 468694



meet the team

Sheena Nagar
Associate Manager

What hobbies/pastimes do you have outside the office?
I meditate most days as I have such a hectic life, it is the one thing that gets me back into balance. I love Pilates and do this as my main exercise. My background is Hospitality so I love being around people and entertaining and socilaising with friends and family. I love listening to music and have a radio in most rooms of my house including the bathroom. And I love travelling.

What was the last foreign country you visited and why?
That would be South Africa which is where I was born. Both my parents are South African and I spend a lot of time there seeing my extensive family. Last year I took a trip of a lifetime and took a sabbatical to travel around Thailand, Australia, New Zealand and Fiji.

What exactly were you working on when you were asked these questions?
I am working closely with the Head of Software Development to assist him in the recruitment strategy in recruiting 3 new IT people into the business. My main role here is to focus on developing the Associate Programme to help us grow and increase our service offerings which will generate another revenue stream for Consult Hyperion.

What was your first job?
I came from a family where you were taught to work hard for your money and pocket money was rare so my first job was when I was 10 delivering the local newspaper on a Friday night.

Who had the biggest influence on your career?
That would definitely be my late father. He was a very driven man who taught me how to be independent and work hard.

If you could change something about the industry what would it be?
Well this is quite contreversial but I would really like to find a way to make recruiters more passionate about what they do. My first job in IT recruitment was with a company called Best who installed strong ethics in recruitment practices and customer service. Under promising but over delivering and managing peoples expectations.

CHYPpings is published quarterly by Consult Hyperion and is avilable free of charge from our web site or by e-mail application to info@chyp.com for the latest issue.

CHYP