[Note: This is the transcript of a podcast dated April 17, 2007, conducted by Dave Birch of Hyperion Consulting. For this and other podcasts, see www.digitalidforum.com.]

DAVE:
Hi, I am Dave Birch from Consult Hyperion. In this podcast we are going to be talking about the use of technology to provide both security and privacy. To discuss it with me I have, quite honestly, one of the world's leading experts on the subject.

STEFAN:
Hello Dave. My name is Stefan Brands. I am with a startup in Quebec in Canada, called Credentica...

DAVE:
... which we have linked to from the blog. Now, Stefan, can I start by asking you how you got into this space?

STEFAN:
Definitely. My background is from academia. I did my PhD in modern cryptography. I started in 1992 in the Netherlands, my home country. I got fascinated at the research institute where I did my work on a research topic that is still preoccupying a lot of professional cryptographers, which is an area we call multi-party security. Which is basically, is it possible to define protocols that involve multiple participants that all have some information, and all of these participants would like to derive some meaningful result from all these individual contributions but they are worried about revealing all their information, and they are worried about attacks (substitution and impersonation attacks and so forth). In this very general setting, can we define multi-party secure protocols.

People have been working in cryptography from the early eighties on that. We know theoretically that anything you can think of can be done in the multi-party secure protocol area. The real question is: can we make these protocols practical. I started in 1992 investigating whether we can do electronic cash payment systems that are secure for everybody, that behave like real cash that you have in your wallet, and that at the same time offer the same kind of privacy protections -- including anonymity where identification is not necessary. Which is one form of security if you think about it.

DAVE:
Now, I remember those early digicash days quite well. I think that was actually where we first met. And I happen to have a paper in front of me right here. I think it may be the first thing of yours I ever read, actually. It's dated 16 October 1994 and is called "Electronic Cash On The Internet." This, as you've said, talks about multi-party security mechanisms to deliver anonymous electronic cash. But I remember there were a lot of discussions at that time about how the technology might be better suited to identity-related applications, in particular things like electronic voting.

STEFAN:
Yes, yes. The stream of research that my research was part of, as mentioned, started really in the early eighties by some brilliant cryptographers. Things like electronic voting, digital credential systems (which today we refer to as identity management systems), access control, and so forth -- they were all part of the same problem space.

DAVE:
And what's critical, what came from that stream of work were mechanisms for people to prove things about themselves without disclosing anything [more] about themselves.

STEFAN:
That is correct, yes. To give you a quick example that sort of started this whole sub-area of research in modern cryptology, there's this famous Millionaire's Problem. You have two individuals who have a certain amount of wealth and they want to find out who of them is the wealthier one without revealing the wealth they have.

DAVE:
So two people who, let's say, sold their shares in their PKI company before the dot com crash want to see who is the richest, and it is possible for them to do that without showing each other how much money they have.

STEFAN:
It is, yes, through a protocol, which is cryptography. Most people think cryptography is about encryption, but encryption has been solved a long time ago, in 1978, and before that using more old-school symmetric key techniques. The real interesting research that has been going on in the past thirty years is all about multi-party secure computation, including authentication in distributed systems. You come up with some kind of problem setting and you want to minimize what different participants reveal to others and minimize the number of avenues for attack; that's crypto.

DAVE:
So how do the millionaires resolve that problem?

STEFAN:
To really understand it you need to understand some number theory, so that gets you into mathematics. But what the early result said was (starting with this problem setting which people then abstracted, but the theoretical result is maybe more interesting) that any problem that you can think of that involves multiple participants that you want to solve, with any kind of security and privacy requirements, if it is solvable by having a central party that is all-trusted by everybody (in the millionaire's setting they both give their numbers to this trusted party who will then say "you are richer") there is a construction that will "virtualize" that central party so that it does not exist. The protocols sort of replace it, so that no one has to trust anyone with anything more than they feel comfortable with.

That is counterintuitive by itself, but it relates to special mathematical properties that are in a way not more counterintuitive than the way encryption works. The fact that I can encrypt a message for you and that you are the only one who can decrypt it (I only need to know a public key of yours), even though we do this in the open, that by itself is counterintuitive. This was the start of modern cryptography, public-key crypto. These techniques you can push further: you can prove knowledge of secrets without revealing them, you can prove properties of secret numbers without revealing what the numbers themselves are. So I can for instance prove that my name is not on a blacklist of suspected terrorists, without disclosing my real name -- which is extremely

counterintuitive. And you know, this is just a little protocol between me and the verifier that has the blacklist.

DAVE:
Incredibly counterintuitive but also incredibly powerful!

So let's just restate where we are in a more prosaic way. So if I imagine a situation where there is me, a giant government database with all my details in it, and the pub, and I am trying to prove to the pub that I am over 18 (or over 37 or however old you have to be to drink in America), what you are saying is: I can replace the giant government database with a cryptographic protocol, and this protocol has the splendid property that I can prove to the pub that I am over 18 without having to tell the pub how old I am?

STEFAN
Yes. In fact it is a cryptographic protocol between me and the government, and one between me and the pub. What it mimics in this particular setting is the digital equivalent of the cards that you have in your wallet. They are issued by trusted organizations that put authenticity marks on them. That could be a government issuing a driver license, which is a set of statements about you. It could have your birth date on it, say. Now the pub, let's say, wants to know "show me from a trusted government organization, that I know and trust, that you are over 18." I then pull out the equivalent of that plastic card from my wallet, my digital wallet, and I just show that my birth date was more than 18 years ago. One of the beautiful aspects of it with regard to privacy is that, instead of showing my birth date which is more than required, I can actually prove that my birth date is more than 18 years ago without revealing the birth date itself.

This is a general principle: I can prove properties of information that, let's say, the government has issued to me in protected form. So I cannot change it, the authenticity marks are there because I am not supposed to modify that. "I am a citizen of the Netherlands," "I am male," "I live in this jurisdiction," "this is my income," "I am with this bank," and so forth, "I am creditworthy," you name it, anything that others could say about me. I can store these statements and retrieve them online in a form that do give me control to reveal only the absolute minimum to relying parties (like pubs, let's say, but it could be other service providers) that need to know something about me to give me a personalized service or to make a better security decision.

DAVE:
So again, just to make it very clear for people, using these kinds of digital credentials with the appropriate protocols, instead of trying to simulate pieces of cardboard, I can prove to the pub how old I am without revealing [more about] my age but also without revealing anything else, my name or address or anything else at all.

STEFAN:
Yes, you can reveal prove the absolute minimum that is necessary to conduct the transaction. If that does include your real name, then you have the option of revealing that.

DAVE:
What other properties do these credentials have?

STEFAN:
Maybe I should not be able to reuse these statements, or maybe I should only be able to use them in certain contexts (like only two pubs in London, right?). It's up to the government: it can limit and restrict whatever I can do with these protected assertions like the cards in my wallet. But it's purely digital. So I get partial control in the disclosure of that information, I am a party to the transaction because I can reveal the absolute minimum that the relying party, the pub in this case, needs to know.

DAVE:
This is how identity cards should work, isn't it?

STEFAN:
In our view (and that includes a lot of privacy activists, some data protection commissioners who are on the forefront of technology, and the cryptographic community that has worked on these things for thirty years) that is the way it should work. Because it's not only more secure for everybody, it scales better. If you think about it, if every pub would have to directly communicate with this one government department in real time whenever I visit a pub or someone else, to find out, "is this person over 18" let's say… [If] the central party (in this case the government department that issues these statements) is not involved in each and every transaction, [this] also increases availability and eliminates denial-of-service attacks, which in an online world are very real, right; if hackers flood the network all of a sudden pubs can't contact the central party anymore in real time, so I may get rejected. Depending on the sensitivity of the transaction that could be a problem; if this is a national defense setting where an access control point needs to know whether I, as personnel, have the rights to access that resource, if it needs to contact in real time a central organization; what if in times of war that gets bombed or it gets taken out of control? What if it is taken over by insiders …

DAVE
… what if it is run by people who are just incompetent and it crashes…

STEFAN
… so there are a lot of reasons why it makes sense, not just for security and privacy, but also for scalability and availability, for me to be able to have a peer-to-peer interaction with the party that I am interacting or transacting with.

DAVE
So a credentials-based approach relies on mathematics rather than on people maintaining a database properly. It delivers more security and more privacy and more integrity and more availability. So obviously this is why it's an interesting way forward. Now, for people who want to look at this, not necessarily for a national scheme, you've now bundled up your implementation of these kinds of digital credentials into a product, haven't you?

STEFAN
Our product is called U-Prove, to remind people that it is really the user proving assertions or facts about him or her, right -- the user is in control. The product is a software development kit, it is really the cryptographic engine that does all these

protocols that we've implemented in the past three years and tested through showcases, with Nokia amongst others. So after three years it is finally done. It is like [the rocket-science component] of a rocket in many ways, that's what the product does, it has to be integrated into solutions.

DAVE
So the product is basically an SDK, and then people are going integrate this into applications. Alright, let's look at an example. Suppose I want to log on to some kind of e-government service. Where would I get my digital credential from, what would it look like?

STEFAN
To sum it up, it is really mimicking the cards in your wallet. It's just digital and it lives on your mobile phone or on your laptop, or maybe on a USB token. Instead of you having to show up at a government office, maybe your mobile phone retrieves these credentials online after you having authenticated. In that sense there is no magic to, and for those of us like yourself who understand PKI and digital certificates, there are some elements that it has in common, other than the elements that prevented it from rolling out. Basically, any organization can act as an issuer of credentials. It's a matter of installing on the server our software or that software package into which our components are integrated. Same for relying parties. It's issuance and verification of just bits and bytes that are protected in special forms and that can be given to users, to their mobile phones and their laptops, and that could be stored on USB tokens and smartcards and whatever you can think of.

DAVE
So let's say the bank gives me a credential that says I am creditworthy or something, or I am resident in the UK. And I want to use this to log on to Ebay or something. But it's just some bits isn't it, in my mobile phone. So what's to stop someone else from just copying it?

STEFAN
I agree. So this is actually one of the reasons why in the nineties these technologies, and that's not just digital credentials but also PKI certificates, haven't caught on because client-side intelligence used to be a bit of a stretch. That's why in early 2000 there was this general recognition that everything has to work with a plain-vanilla browser, which can only do so much. It cannot have special protections in there. That's why we have sort of started to drift into an electronic world where everything about you is really done in the back-end, directly between organizations, which therefore can track and trace you and have impersonation powers and so forth. Now that we have these mobile phones…

So there has to be client software on here and it may ultimately tie into tamper-resistant chips, depending on let's say transferability, which is one example; what if I am not supposed to transfer myself my own credentials to my neighbor. If transferability is a problem then the issuer, the government organization let's say, could say "we're going to issue these credentials to a tamper-resistant smartcard." There we have special techniques so that you can extremely efficiently do that, avoiding a lot of the current problems with attacks on smartcard chips and the cost of the chips.

The other is, for instance, we can issue to Dave a digital credential that has some information in it that is confidential to Dave himself. The implication is that when you use your digital credential you will never show the information that the issuer put in there (maybe it's your credit card information); you can do that, this is part of the selective disclosure techniques. But if you wanted to give me a copy of your digital credential, you would need to reveal the information to me that you would rather not reveal, because otherwise I cannot use your credential. So these are special techniques that are kind of counterintuitive.

DAVE
Which is one of the things that makes them hard to explain to people, isn't it, even though they are very powerful. Do you feel that these kind of privacy techniques are starting to get a hearing now?

STEFAN
Depending on the market that we are talking about, the awareness of all kinds of sensitivities with regard to personal information has certainly gone up a lot in government contexts and in the financial industry because of all the breaches. So there is a growing awareness that if as an organization we don't need to have certain information, if we don't strictly need it on our customers, it is better not to collect it in the first place. It is starting to happen, yes.

DAVE
It is starting to happen, that's true. Thank you very much for your time Stefan.