

June 2005

e-passports: Interview

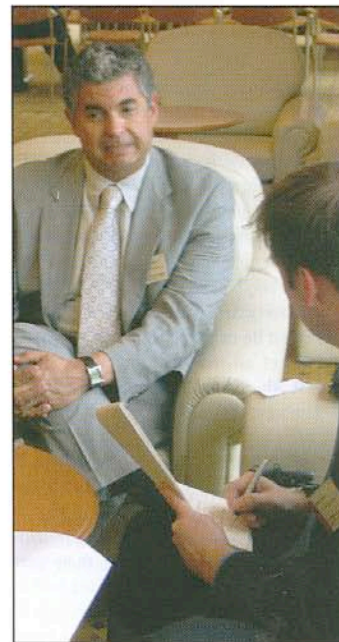
Secure validation - anytime, anywhere

In access control applications involving millions of users, authenticating identity has become a relatively simple process, while validating a person's privileges, just as critical to avoid loopholes, may require a new approach

Authenticating the identity of a person presenting a secure document or token is crucial, but just as important is to validate whether that person is allowed to access the network, facility or even country. With initiatives emerging on a global scale, such as the e-passport, it becomes increasingly difficult to successfully validate billions of users using traditional network and database architectures. There is however another way...

It is no coincidence that a small group of talented engineers made the decision to form a start up company – CoreStreet – in the immediate aftermath of the September 11 terrorist atrocities. Phil Libin, a member of the original team, and now president of the Cambridge, Massachusetts-based company, explains that, "We all felt that we wanted to do something consequential and meaningful. So we started the company on October 11th, 2001 – exactly one month after the attacks." The 12-strong engineering team had been working together for around 15 years and, upon joining forces with famous MIT cryptographer Silvio Micali, was able to start CoreStreet with a strong portfolio of 13 patents. There is no doubt that since it started up, the company's technology has been creating a stir in the identity world.

Defining exactly how CoreStreet approaches the validation question, however, is not a simple concept, in the way that one can more easily imagine how validation operates online across networks connected to central databases. To understand where CoreStreet is positioning itself, it is necessary to consider the two questions that need to be addressed when any secure transaction takes place. First it must be established if a person is who they say they are. This is the authentication step and most often involves passwords, biometrics, PIN numbers, digital certificates and secure tokens. Once this is established, the next question addresses whether that person is allowed to do whatever they are trying to do? This is the validation step.



Phil Libin, president of CoreStreet (left) and Ayman Ashour, co-CEO of Assa Abloy ITG (right), during the interview

According to Libin: "If you look at these two major steps, the difference is that identity is fixed (even if I become a terrorist and all my privileges are revoked, I am still the same person), but validation changes with time. You need both, however, in order to have a meaningful infrastructure." This second question has been largely ignored - to the detriment of real-world security, according to CoreStreet. The problem is that traditional validation techniques require connection to centralized databases. This is fine for relatively small numbers of users, but tends to break down in large and geographically distributed deployments.

CoreStreet contends that there is no practical way for millions of users from all over the world to connect quickly and securely to a centralized

system billions of times a month. And yet, it points out, those are precisely the requirements for today's largest security applications, such as e-passports or government ID schemes. Such a validation scheme may be possible, but could cost millions of dollars and would most likely be complex and slow. Therefore, CoreStreet says, many organizations have chosen to skip this vital step, resulting in worrying holes in security.

An alternative approach to validation

According to CoreStreet, its technology allows any number of users and transactions to be validated instantly, without the need for constant

connectivity and secure infrastructures. In other words it becomes possible to know whether any action should be allowed to happen even without having access to a network. This, the company claims, reduces the total cost of security systems by as much as 90% and makes response times fast enough so that legitimate users are not inconvenienced by the security.

At the heart of CoreStreet's technology is the idea of a 'self-validating proof'. These proofs, or Real Time Credentials, are short messages embedded with information for validating and authorizing certain activities and access permissions. CoreStreet proofs are small, very fast to compute, and do not contain any secret or sensitive information. Cryptographic techniques are also used to ensure that the messages cannot be forged or modified by any unauthorized party. According to CoreStreet, because these messages can be trusted even if distributed across unsecured networks or media, most of the traditional cost and complexity issues associated with Public Key Infrastructure (PKI) systems are eliminated.

Always available

One of CoreStreet's main licensees, Assa Abloy's Identification Technology Group (ITG), is enthused by the potential that CoreStreet's products bring to the large-scale identification market. According to Ayman Ashour, co-CEO of ITG, "There is a lot of excitement in the IT world about what CoreStreet can do. For us in ITG, the excitement is when you are talking about a single credential working across multiple systems doing multiple transactions. And the beauty is that not all these systems have to be online." As an example Ashour highlights the case of a cockpit door in an aircraft. "It is not connected to anything, it is completely standalone. We can use CoreStreet's software to record on the authorized pilot's card that some other person's authorization has been revoked and is not al-



lowed access. When their card communicates with the door reader it feeds it that information." In fact, as Libin points out, "It goes further than whether the solution works online or offline. It has to work everywhere, all the time. For identity to make sense it has to keep working when everything else stops. Your identity has to stay up and running not only when all your networks are working perfectly, but also when there is a natural disaster or a terrorist attack."

Passport sector

An obvious application area where CoreStreet's technology could provide a significant input is in the fast-moving e-passport sector. According to Libin: "Most people today, quite rightly, are addressing the question of how we create these new electronic passports – how do we print them, make them hard to forge, make them interoperable with passport readers and so on. Not a whole lot of people are talking about the second question, which addresses the rest of the network. CoreStreet technology can play a role in the validation of passports so that every single time a passport is scanned, no matter where it is, the passport examiner can instantly, without waiting for any sort of connectivity, know whether that person is valid, has the appropriate visas, is on any watch lists, or whether the passport is stolen. So all of the dynamic information you want to know can be available regardless of where you are in the world without the need for any large, vulnerable centralized databases."

In the passport application, authentication information will be stored on the chip in the passport – as is currently the case. However, the validation information can be stored in many places. Libin explains that the CoreStreet proofs can exist on the network, the passports themselves or the readers, "So we've got a sea of digitally signed validation information," he said.

As an example of the work CoreStreet is doing with Assa Abloy ITG, halfway through our interview with Libin, he pulled out from his bag a prototype handheld Windows CE-based reading device. "There are 14 million CoreStreet proofs in here – and its maybe 3% full. You could easily fit a database of one billion people in here. The size of the data involved is one of the things that we do better, so we can manage validation data for hundreds of millions of people very practically."

Applications

If a person loses their passport or reports it stolen, the document needs to be revoked. Similarly the passport needs to be cancelled if it is discovered that a person has managed to obtain an authentic passport through the use of falsified breeder documents. Libin says that CoreStreet's technology has the power to distribute this revocation proof for any number of passports, without the possibility of modification whilst it is in transit, and without having to connect to a central database. This would allow the passport examiner to know immediately whether any particular passport was valid or not. According to Libin, "At the very least we should do that and do it well, so that if a passport is reported stolen then there is an almost zero chance that any passport reader would say it's valid."

Whether a CoreStreet solution in the area of passports will be implemented in the near future is uncertain, because the passport industry is renowned for its conservative nature when implementing new technology. Nevertheless, the groundwork has been laid for CoreStreet's technology through the introduction of smart card capabilities into the passport document, and as time moves on it could become clear that such a solution is needed.

Implementation

While the passport market might take some time to crack, ITG's Ashour believes that the technology could be used in the e-visa market in a much shorter timeframe. He comments: "If we look at the USA where the whole e-passport program started, then this really applied to the visa-waiver countries. A natural step is going to be an e-visa for the non visa-waiver countries. e-visas will enable governments to include specific information, such as your date of application, what you said when you applied, your access privileges and so on. Here the CoreStreet technology could make an impact in the short term."

Whatever the application, Libin is keen to stress that authorities don't have to do anything different today, in order to use CoreStreet technology later on. "We are not advocating any changes to hardware or software or to introduce any additional complications. We will be ready to provide some neat ways to solve a lot of problems when countries start to use passports and visas on a large scale."

by Mark Lockie