



Enabling End-to-End Trust in the Digital Transaction Age

*Randy Vanderhoof Keynote Address
CTST 2009 Americas Conference
May 6, 2009*

Abstract

Cell phones, digital transactions and the Internet have transformed the way we interact, but also made identity, payment and other information more vulnerable. In this luncheon keynote, Smart Card Alliance Executive Director Randy Vanderhoof, named one of the 25 most influential people in the security industry, demonstrated why advanced card technology is the best way to enable end-to-end trust, all the way from the hand of an individual to any system or organization. He examined the trend toward personal digital security to protect identities, transactions and information in banking, government, mobile communications, healthcare and transit and projected how the rising tide of cybercrime will drive the next wave of business opportunities for smart card technology—person-centric digital security.

➤ [YouTube Did You Know 3.0](#) video

Good question, right?
What *does* it all mean!

We have Karl Fisch & Scott McLeod & Jeff Brenman – and I guess Steve Chen and Chad Hurley – the founders of YouTube – to thank for helping us realize just how little we really know about the dynamic world we live in. Since I became aware of that video, I have learned that it has been viewed over 2.5 million times so I hope it was new for at least some of you in the audience today.

That last stat in the video - that 600 hundred thousand illegal music downloads occurred during the presentation – is pretty scary if you are in the business of making records, TV broadcasts or movies. They are getting ripped off almost at the speed of light!

Well, that got me thinking about what I wanted to share with all of you today about building end-to-end trust in digital transactions and we did a little research of our own. We discovered some pretty scary statistics that are a little closer to home for those of us who are here today and who are in businesses other than the security of digital music downloads

Information security is a big business. \$6.8 billion is being spent just on the network security piece, according to IDC, and that's just part of the pie. There are thousands of great products available for information security. These systems encrypt data, store data behind firewalls, and send it digitally scrambled as it moves from place to place. Everyone uses it and every IT person is aware of why they need it. So everything must be great right?

No. The evidence shows cybercrime in all its flavors is increasing not declining.

Clearly, despite all the efforts to focus on data pipelines and firewalls and intrusion detection and expensive industry initiatives to audit data security processes and finally even bigger central management consoles that roll up all of the pieces to try to make this patchwork of solutions manageable.... despite all of that, the problems are getting worse.

In my view, we have to turn all of this on its head. The answer is not more and better walls around the data. The answer is **putting identity security first into the networks that manage that data.**

What do I mean by this concept putting identity security first? My point is that with the focus on data and pipeline security, we are not making enough effort to strongly authenticate individual identities either in information systems or over financial networks that process our transaction data.

By putting identity security first, we can solve many problems involving stolen information, fraudulent transactions and identity theft -- problems that cut across many applications including banking and payment, healthcare services, Internet-based services, and enterprise and government-wide information access.

The vast majority of information systems still rely primarily on usernames and passwords for identity authentication. This, despite the fact that if someone can steal your username and password, they can get into your account, whether for banking, payment or your employer's information systems, where they might be able to steal personal information records by the thousands. Why? Because by making it harder to weed out the criminals by adding a second factor of authentication, we "tax" the everyday non-criminal user or business owner with added cost or added inconvenience. Either case creates "friction" in our digital communication superhighway.

Two examples of this kind of identity problem are payments systems and healthcare systems.

Payment systems, both online and at retail stores, rely on static account numbers issued to credit-worthy individuals to identify those individuals in payment transactions. This seems to be adequate for the most part for face-to-face payments, but it creates a big hole for unattended sales like pay-at-the-pump gas stations and for all of those card-not-present online transactions on the Internet or the home banking web sites that allow us to transfer funds and send checks -- that are only protected by a user name and password. With billions of transactions flowing through the systems and millions of end points to secure, basing security on stronger data security measures to safeguard these static account numbers or protecting access to our personal financial accounts with just passwords seems to be an unsustainable approach to security in these times.

Hospitals and other healthcare providers continue to require redundant and repetitive entry of personal, insurance and medical information by their patients, even in the same facility -- and even for repeat users of the same facilities. This can lead to identity errors that can have the most serious of consequences -- accidental death, caused by getting inaccurate information in the patient record, or even having the wrong records. Health identity theft and insurance fraud are also growing problems because it is so easy to beat the system -- or lack of a system -- that is in place today. Major reforms are coming but there is no silver bullet to fix the healthcare industry.

The threats to everyday citizens on the Internet are well documented.

Phishing is a challenge for an increasing number of shop-at-home, bank-at-home, and information-“surfing”-at-home users. Even the most Internet-savvy users can become victims. Phishing has become a “National Sport.” Whether from an email or a program that redirects you to a phishing site, the number of attacks remains at all time highs, and still victimizes millions.

We have seen spectacular data breaches involving millions of stolen account records. The cost is not only measured in actual fraud resulting from such breaches, but also the cost of consumer confidence, merchant reputation, lost sales when cards need to be cancelled and reissued, lost hours of reporting fraud to the banks to recover funds or remove charges, damaged credit rating, and much more. Causes range from weak network security, to failed software safeguards, to stolen passwords, to simple negligence.

Spyware and malware have become rampant over the Internet. Long gone are the days of dial-up Internet sessions that lasted only minutes or hours. Now we have high-speed always-on connectivity with unlimited data access and bandwidth accessing an ever-greater volume of music and video. Spyware is aimed at stealing either passwords or payment account information or both. Things call “Botnets” anonymously distribute keyboard loggers, file downloaders, financial Trojans and other malware that steal identities and accounts, one at a time or in bulk.

If you think you have safety in numbers – think again. Spyware can look at programs and files on your computer and frequently visited web sites – like online brokerage accounts – and look for high value targets out of the masses. Since everything you type on your keyboard – like passwords and URLs – even if it connects via a secure Internet channel later, is in the clear as you type it and is vulnerable to keystroke logger programs. Solutions require better anti-spyware plus the introduction of a strong second factor when we login to a web site.

So it all comes down to what is missing in our digital transaction world - **Identity Security**. But how big is the problem, really? We did some research of government and industry sources and what they say about these challenges we face – and we put together our own video version of “Did You Know” to help bring this point home – take a look

➤ [Smart Card Alliance Did You Know](#) video

What all that means is we have to start **putting identity first**.

Identity is something that is definable, that includes a set of qualities or characteristics that distinguish one individual in possession of those qualities from other individuals with other qualities or characteristics that can be recognized electronically. We call these qualities, attributes. Identity attributes, to be used for access, need to be authenticated by some authority so that someone can assign privileges to those individuals who possess those approved attributes. Proof of identity is associated with access, but it's not just access. Putting identity first also means more strongly protecting people's identity by making our transaction systems reliant on the will of the person initiating the transaction to release that identity information – so personal control and responsibility are added to the transaction.

Proof of identity is associated with access, but protecting identity is associated with guarding against another person misusing my identity or any type of privileges assigned to me, whether it's my credit card line or my healthcare insurance.

We live in a digital age. With more systems, more interconnections, more complexity. We have more channels, more speed and more mobility, More devices and more ways to work and pay and shop. And people are carrying electronics with them everywhere they go. We all know that.

So why is it we still mostly use the most basic techniques to protect people's identities, assets and privacy?

Passwords. Static account numbers and security codes. Magnetic stripe cards.

Yes, in a world awash with cybercrime our idea of identity security is based on the technology equivalent of an eight-track tape.

We have to put an end to the idea that all we need in the hand of the consumer is a pointer – a record locator number – that points to something else. That thinking goes hand-in-hand with the data fortress mentality, the concept that security only matters inside the perimeter of the payments network (in the servers and storage devices), not at the edge of the network. The card that represents my identity at the POS terminal has to start to play an active role in protecting my identity – like waiting for me to enter my PIN or biometric instead of just relying on a successful swipe of a mag stripe . We have to stop thinking – or more accurately, hoping – that after a card is swiped, we just need that one more patch to the server, one more analytics check in the network or one more security policy to solve the problem.

If we are going to meet the challenge of managing and protecting identity in our digital age, we have to bring personal digital security technology all the way out to the hands on the consumer.

If we are going to meet the challenge of managing and protecting identity in our digital age, we have to introduce personal digital security technology that can actively help protect access to identity information, as well as the integrity of transaction systems that manage the digital identity information. Not just point to a record.

If we are really going to put identity first, we are going to stop thinking of fraud and identity theft as a cost of doing business, and start considering it as a fundamental responsibility of the trust our customers place in us. It means getting to a place where just stealing someone's account numbers or passwords cannot give a criminal the means to defraud that individual.

The best way to achieve all of these goals is to make the edge of the digital transaction – the part that starts with one's personal identity attributes – SMARTER. Using smart card technology is a proven way to do it.

Smart cards can provide the best end-to-end identity security because they are computing devices. With its self-contained microprocessor and software, smart cards put digital identity security right in the hands of the consumer.

A digital data signature can prove the authenticity of the device and its contents. Challenge-response techniques with random, dynamic, transaction-specific inputs provide bi-directional

authentication for access. This is done on-board the smart card, making it possible to confirm any reader device with which it connects and eliminating the need to even trust the device at the edge of the transaction network. Communications can be encrypted. Dynamic, unique transaction signatures can establish irrefutable evidence of card presence, anywhere, anytime, on any transaction network. Smart cards can make security decisions based on the time and location of the transaction, like attempting a card plus PIN plus online authentication first, and if that is not available, making the decision if it will accept a less secure card plus PIN plus offline authentication based on the merchant type or dollar amount.

Of course today's smart cards aren't always cards. They are SIMs, USB tokens, epassports and soon contactless tags. But in all its forms, smart card technology is ideal for identity security.

Many countries in the world have turned to EMV smart cards to secure payment transactions. Canada is committed to migrating parts of its debit networks to EMV by 2010 and its credit networks soon after. Canada is already deploying cards and acceptance infrastructure.

So is Latin America, as we learned at last year's CTST the Americas and as you will hear again during today's CTST track session on Latin America. Mostly it is driven by a big uptick in fraud losses due to cloning and skimming, which grew in Brazil at a compounded annual rate of 43% from 2004 to 2006, according to one of the bank speakers at last year's conference

Europe is now starting to use their EMV cards more widely for online transaction security as well.

In the United States, however, if there is any serious discussion taking place here of how EMV or anything comparable could benefit stakeholders, it is a well-kept secret. Nonetheless we did get the support of at least one important individual, the vice chairman of TJ Maxx, who stated in an interview last year with the Boston Globe that we need to get to a point where stolen account numbers and security codes are not a threat to consumers, issuers or merchants. He also correctly stated that smart card technology can help get us there. I would like to see more activity at the Smart Card Alliance directed to re-examine options for using smart cards to better protect payment transaction networks in the United States.

Healthcare is another application that can benefit from a focus on identity security. As you saw in the video, there are real costs to this industry due weak identity management. The American Recovery and Reinvestment Act is calling for dramatic reforms in healthcare IT systems, while further empowering individuals to take control of their most sensitive personal information – their health information. Much emphasis has been placed on the need for electronic health records for every American, and ways to exchange those records at the regional, state and national levels.

But this is putting the emphasis on the wrong part of the problem. Such an effort must start with the accurate identification of each person receiving healthcare services or participating in healthcare benefit programs. Next, there must be a way to uniquely and securely authenticate that person across the healthcare system, including over the Internet, in a secure and privacy-sensitive way. Our policy makers and industry leaders need to give people the health identity tools that will let them manage their health data and protect that data from the same dangers that threaten the security of our financial data and leave people vulnerable to stolen identity information.

Healthcare stakeholders, especially, need to take identity security seriously. On April 16, 2009, the FTC published a proposed breach notification rule for electronic health information -- the proposed rule that would require entities to notify consumers when the security of their electronic health information is breached.

The Smart Card Alliance Healthcare Council and Identity Council are actively addressing these needs. We are working hard to get the healthcare industry to put identity first, and to understand that smart cards are the best end-to-end solution. We need to work extremely hard to get this sector to start out on the right foot with smart card technology.

Part of our activity includes recognizing the contributions of leading organizations and individuals who are putting smart card technology to work protecting identities and transactions with our awards for Outstanding Smart Card Achievement, or OSCAs.

I was pleased to see Mount Sinai Hospital receive the Outstanding Issuer Award this year for their pioneering efforts in Personal Health Cards -- an industry model for putting identity management at the front of the electronic health record evolution. Also, HID Global received the Outstanding Technology Award for its work in incorporating multi-technology contactless readers into Dell laptop computers to further integrate two-factor authentication security into personal computing and speeding the elimination of user names and passwords. Lastly, our Individual Leadership Award winner, Patrick Hearn, from Oberthur Technologies, helped advance the government PIV interoperable identity standard and led his company's efforts to supply FIPS 201 certified cards to the government. These organizations and individual leaders are what this industry needs more of to move the identity security movement ahead.

Returning to this theme of putting identity first - we also need to address **personal responsibility**.

Putting identity first also means involving individuals in their own identity security. Individuals have the most to lose, and we collectively as service and technology providers have to expect them to take more responsibility for protecting their identity.

People recognize how much information is out there, but they also feel powerless to protect it. We have to hand them personal digital security devices that can empower them to better protect their identity, personal information and privileges.

Certainly people also have a resistance to carrying something else, but they cannot have it both ways.

If we are going to put identity first, and evolve our information systems and transaction networks to be resistant to attacks, than simple, easy-to-use authentication methods are essential -- and people have to play a role.

If the best way to provide end-to-end security is with a personal identity device based on smart card technology that can provide active strong authentication for access or in transaction systems, people will have to carry and use that device. And they will.

Or maybe people will just use their cell phone. The fact that Verizon, the market leader, is moving into smart card technology too is certainly good news for our industry, and the presence of the smart card, called the UICC, in so many phones creates interesting possibilities.

With SIMs, the smart card and the SIM subscriber application were really closely bound together. The next generation SIM is the UICC and it is designed to have multiple applications.

While the UICC's main mission is mobile telecom, it also may create new ways to put identity first in other sectors as well. Those of you like me who were here in the '90s remember the mantra of multi-application cards. But we were stymied in finding the "killer app" that would put smart cards in everyone's hands.

Well, mobile devices look like they can be the game changer in this market, and the UICC may just turn out to be the personal multi-application solution we envisioned in the '90s.

Phones are already being used for out-of-band authentication, where your bank calls you at home or on your cell to give you a one-time password to set up web access to your bank account for example. Why not create UICC applications that can better secure identity access and transactions by using your mobile device to communicate that information?

But whether it's in your cell phone, your bank card or something else, people are also an essential part of putting identity first.

So, this long way of making the point that identity and identity security are the answers to enabling end-to-end trust in the digital transaction age needs to come to an end so that you can get on with your dessert and the rest of the conference agenda.

But let me close by thanking my colleagues in the Smart Card Alliance. The Smart Card Alliance is not any one organization, or one individual who has scripted the way the world has responded to the challenges of the digital age. These words and the words of many of the speakers here this week became absorbed and processed through the interaction of hundreds of individual voices and written words that have been cultivated through the discussion group calls of the councils, the web seminars, the white papers and the press announcements generated by the Alliance participants. The justification for most members to pay their dues and to lend us their talent for the various projects we lead is to raise the market for all players and therefore raise the value of each player's share of that market to a degree greater than they could effect that change on their own.

I think we are achieving that justification by the tremendous growth in smart cards across multiple vertical markets. It is at events like this one, our Annual Conference, and together with CTST, that it becomes ever clearer to me – and hopefully to all of you – about how far we have come as an industry and how much respect our industry has gained within the government and payments, and healthcare and security, and mobile markets that we are suppliers of technology and services to.

Thank you everyone for your support for me and for the Smart Card Alliance and the smart card industry -- for furthering our cause of "enabling end-to-end trust in digital transactions."