Femtosecond®
www.femto-second.com

In the News

Volume 1 Issue 16

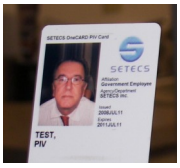
July 13, 2008

Commercial PIV Status

By now many hoped for commonality in identification. Yet there seems to be a multiplicity of ongoing efforts including the Personal Identity Verification (PIV) card, the Travel ID, Real ID, and others. Some politicians supporting a common ID are now revolting against approached such as Real ID [1].

Lab Testing Commercial PIV Capabilities

The PIV process is well documented for Federal customers and support contactors. But what of volunteers and others, that interact with the Government on a not for fee basis? The cost for a background investigation and the time required for completion are obstacles for many agencies. Consider volunteers that need to enter Government buildings but are not contractors. Does it make sense to have them undergo a background investigation? The concept of a Commercial PIV capability was discussed by Judith Spenser at the last Interagency Advisory Board (IAB) meeting. The commercial vendors are not allowed to issue their own Federal Agency Smart Credential Number (FASC-N) and would need to comply with certificate provider requirements that are cross-certified with the Federal Bridge CA. Still, there is a real requirement to have greater Government interoperability. To address this need, work continues on developing a commercial PIV capability with the objective of interoperability with the Federal PIV community.



The key to an interoperable solution lies in the trust relationship to the common policy CA. For cryptographically bound trust, there must be a validated path to the common policy CA. For many, the Federal Bridge CA offers a cross-certification path. As commercial entities satisfy the Policy Authority requirements, it is expected there will be more interoperability. This will become more critical as more agencies migrate to the PIV card and the infrastructure that uses these cards.

For commercial efforts, such as Commercial PIV, the vendors will

(Continued on page 2)

Financial News

This week, The Office of thrift Supervision transferred the IndyMac Bank to the FDIC [1]. The FDIC estimates the cost to its insurance fund will be between $4 to 8 billion [2]. Regulators are calling this the bank's failure the second-largest in U.S. history [3]. Reports are blaming the run on the bank due to comments made by the chair of the Senate banking committee [4]. Reports suggest the OTS is blaming the senior senator's letter on the stability of IndyMac as the reason depositors pulled their money out of the bank [5]. Furthermore, IndyMac has been in the news involving mortgage fraud. For example, in Sacramento five people were indicted on mortgage fraud for submitting dozens of fake loans at Aegis Mortgage and IndyMac Bank [6]. In Michigan, a real estate broker

(Continued on page 2)

Inside this issue:

Fed News	2
Fannie and Freddie	3
Bank Fraud	3
Medically Wired for Hackers	4
More Security Vulnerabilities	4

Special points of interest:

- Implanted Pacemakers and defibrillators vulnerable to hackers
- Two compromised passwords almost resulted in 90 million euro loss for HSBC bank
- Regulators take over second larges bank failure in US history

Poorly Written Software that Kills

(Continued from page 1)

need to work closely with the digital certificate providers to ensure that all requirements they need for Federal Bridge interoperability are satisfied at the local registration and issuance side.

Most of the current physical access control systems are not path validating the digital signatures so creating bogus cards could be a near term problem. Until the physical access vendors start verifying the integrity of the cards through path validation, PIN with biometric and contactless authentication will have some exposure to fraudulent credential.

1. Carney, Eliza Newlin, National Journal Magazine, *Identity Problems*, July 5, 2008.

Fed News

The Federal Reserve will be issuing new lending rules that restrict exotic loans [1]. This comes at a time when lawmakers are aligning to support increased powers for the Fed [2].

In other news, the demand for emergency funds from the Fed has declined [3]. In an effort to make refinancing easier, the Fed plane to bane loan penalties on high cost loans [4].

1. Labaton, Stephen, The New York Times, *Fed to Clamp Down on Exotic and Subprime Loans*, July 9, 2008.
2. Robb, Greg, Market Watch, *Scales tilt in favor of Fed getting new powers*, July 10, 2008.
3. Chicago Tribune, *Demand drops for emergency lending by Federal Reserve*, July 11, 2008.
4. Vekshin, Alison, Bloomberg, *Fed to Bar Loan Penalties That Deter Refinancing, Person Says*, July 12, 2008.

Absence of evidence is not evidence of absence–Dr. Carl Sagan

Financial News

(Continued from page 1)

was charged in a $20 million scam that included a $130,000 loss to the IndyMac bank [7].

Oil hit a new record high passing $147 per barrel [8]. With the high cost of oil, we would expect a dismal trade deficit. However, the trade deficit decreased by 1.2 % to $59.8 billion while the deficit with China increased from $20 to $21 billion [9].

In other news, the Senate passed the mortgage foreclosure rescue bill that will provide up to $300 billion to help approximately 400,000 homeowners [10].

1. Veiga, Alex, Associated Press, Office of Thrift Supervision shuts down IndyMac, July 11, 2008.
2. Reuters, *Regulator to run IndyMac while buyer sought*, July 11, 2008.
3. UPI, *U.S. takes over IndyMac Bank*. July 11, 2008.
4. Reuters, *IndyMac seized as financial troubles spread*, July 13, 2008.
5. Bower, Jerry, CNBC, *How Chuck Schumer Caused the Second Largest Bank Failure in US History*, July 12, 2008.
6. Associated Press, *Five indicted in alleged Calif. mortgage fraud*, June 28, 2008.
7. Mickle, Bryn, The Flint Journal, *Former Grand Blanc Township real estate broker charged over alleged fraud*, June 19, 2008.
8. Cooke, Kristina, Reuters, *Fannie and Freddie fears, oil over $147 hit Wall St*, July 11, 2008.
9. Aversa, Jeannine, AP, *Trade deficit ebbs as exports rise to record high*, July 11, 2008.
10. Davis, Julie Hirschfield, Associated Press, *Senate passes foreclosure rescue*, July 11, 2008.

Fannie and Freddie

Fannie Mae alone guarantees $2.8 trillion worth of mortgages [1]. Rumors started to spread Monday on Wall Street that Freddie Mac and Fannie Mae were in trouble [2]. There are reports that the Government is considering taking over Fannie Mae and Freddie Mac [3]. If either of these mortgage giants is found to be undercapitalized, a1992 law would allow either to be put into a conservatorship [4]. Lawmakers have been quick to support a government bailout of the home loan buyers [5]. The talk of a Government bailout of home loan giants has had the negative effect of driving down their stock prices [6]. In an effort to dispel rumors, the Fed has not had any meeting with Fannie Mae and Freddie Mac to discuss direct loans from the central bank [7]. However, others suggest $15 billion is being considered [8].

1. Benner, Katie Fortune, *The Fannie and Freddie doomsday scenario*, July 10,2008.
2. Duhigg, Charles, Houston Chronicle, *Fannie, Freddie see woes mount*, July 10, 2008.
3. Plumberg, Kevin, Reuters, *Government considers Fannie Mae, Freddie Mac takeover: report*, July 11, 2008.
4. Market Watch, *U.S. weighs Fannie, Freddie takeover: report*, July 11, 2008.
5. Kopecki, Dawn, Bloomberg, *Fannie, Freddie Too Critical to Fail, Lawmakers Say*, July 11, 2008.
6. Zibel, Alan, Associated Press, *Freddie, Fannie shares down on talk of gov't aid*, July 11, 2008.
7. Lanman, Scott, Bloomberg, *Fed Says No Talks With Fannie, Freddie About Loans*, July 11, 2008.
8. Dey, Iain, and Rushe, Dominic, Times Online, US Treasury rescue for Fannie Mae and Freddie Mac, July 13, 3008.

Bank Fraud

As the financial markets continue to fluctuate, more cases of bank fraud are in the news. The former CEO of First Bank Mortgage, was charged with fraud resulting in a $35 million loss [1]. Allegedly, the losses started back in 1987 and the fraudulent activities were concealed [2]. The former chairman of Westar Energy Inc is appealing a 2 year imprisonment sentence for bank fraud exceeding $1 million [3]. In Mississippi, a former real estate developer pleaded guilty to conspiracy to commit bank fraud trying to secure $14.5 million from 20 banks [4].

In west Virginia, BB&T was bilked out of $6 million by a former car dealer convicted of bank fraud [5]. The convicted man was order to pay almost $4.3 million in restitution [6]. It seems there is at least a $1.7 million loss.

Perhaps the best example comes from the United Kingdom. Apparently, a man who stole co-worker's passwords made a mistake and was caught transferring 90 million euros [7]. A key point here is the use of passwords. Reports indicate that two of bad actor's colleagues, passwords were used to carry out and approve the transactions [8]. So how long will financial institution continue to rely on passwords for identification and authentication?

Elsewhere overseas, 9 people have been convicted of $1.9 billion fraud at the fourth largest bank in Austria [9]. Reports indicate risky loans were made to U.S. futures trader Refco Inc shortly before they went bankrupt [10].

1. Volkmann, Kelsey, St. Louis Business Journal, *Former First Bank Mortgage CEO Turkcan indicted on wire fraud, faces prison*, July 10, 2008.
2. PRNewswire, *Former President of First Bank Mortgage Indicted on Multiple Fraud Charges Causing a Loss of $35 Million*, July 10, 2008.
3. Wichita Business Journal, *Wittig appeals ruling on bank fraud sentence*, July 7, 2008.
4. Strange, Ashley, WJTV, *Bank Fraud*, July 7, 2008.
5. WSAZ, *Former Car Dealer Sentenced for Bank Fraud*, July 10, 2008.
6. Clevenger, Andrew, Charleston Gazette, *Ex-car dealer gets 26 months in bank fraud*, July 11, 2008.
7. Finextra, *HSBC clerk gets nine years for attempted £72m fraud*, July 9, 2008.
8. BBC Mews, *Clerk jailed for £72m bank fraud*, July 5, 2008.
9. Kole, William J., Washington Post, 9 convicted in Austria fraud case, July 5, 2008.
10. Reuters (UK), *Austria court convicts bankers over heavy BAWAG losses*, July 4, 2008.

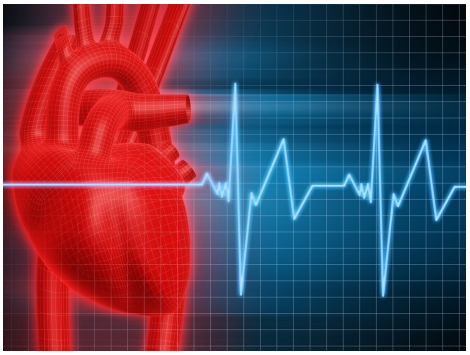
Plan your work for today and every day, then work your plan– Margaret Thatcher

Medically Wired for Hackers

It reads like a horror story, a hacker finds a way to control a heart pacemaker. Each year, approximately 160,000 defibrillators and 250 000 pacemakers implanted [1]. Researchers have determined that such devices, relying on wireless technology, are vulnerable to hackers [2]. So as if having weak web security were not bad enough, millions of Americans could be at risk to hackers.

Among the recipients of an embedded defibrillator is our current vice president, Dick Cheney [3]. Estimates are that up to 25 million Americans have at least one implanted medical device [4]. Others include devices such as drug dispensing pumps.

Our reliance on technology



without adequately assessing the security risks continues. While there are no reported cases of hacked pacemakers, now that the vulnerability is known how long will it be before security is added?

1. Karlin, Susan, IEEE Institute, *Hacking Hearts*, July 8, 2008.
2. Halperin, Daniel, et. al., proceedings of the 2008 IEEE Symposium on Security and Privacy, *Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses,* 2008.
3. USA Today/AP, *Cheney leaves hospital after tests*, November 13, 2004.
4. WSCO (Charlotte), *Implanted Medical Devices*, June 20, 2008.

In preparing for battle I have always found that plans are useless, but planning is indispensable– Dwight D. Eisenhower

More Security Vulnerabilities

For month, vendors have been working on a DNS patch (released last Tuesday) that would have allowed hackers to control Internet routing [1]. What is interesting is that the work to correct the problem was coordinated in secret [2]. The DNS vulnerability illustrates that once a vulnerability is discoed, the fix may take time. Along the same lines, the OS X 2.0 update for iPhone was released last week and includes security fixes for one problem that has been an exploit since last February [3].

Microsoft released stopgap instructions for users of Internet Explorer that hackers have been exploiting to break into computers [4]. Additionally, there is report that Microsoft Word 2002 service pack 3 has an exploit that is activated when web users open a word document saved with this version [5]

The hackers are getting their attacks out early and often. The frequency of security patches points to the need for a good patch management process. The real challenge is how to better protect the home users that are seeing their computers compromised? What is the cost of security in maintaining ever increasing security patch management?

In other news, a high school student hacked into the school and discovered teachers' salaries and medical records [6].

1. Chapman, Glenn, AFP, Internet flaw could let hackers take over the Web, July 9, 2008.
2. Keizer, Gregg, Computerworld, *DNS researcher convinces skeptics that bug is serious*, July 11, 2008.
3. Krebs, Brian, The Washington Post, *A Baker's Dozen of Security Updates for iPhone 2.0*, July 11, 2008.
4. Krebs, Brian, The Washington Post, Microsoft: Hackers Exploiting Unpatched Office Flaw, July 7, 2008.
5. Leffall, Jabulani, Redmond Channel Partner, Word 2002 SP3 Subject to Remote Attacks, July 9, 2008.
6. Rozek, Dan, Chicago Sun Times, *New Trier hacker saw teacher salaries, medical records*, July 10, 2008.