"e-Agriculture" — The Farm and the Internet

by:
Don Rhodes

Today, many farmers currently wait in long lines to file USDA paperwork at county offices. The American Farm Bureau estimates that farmers spend about $20 million annually to comply with federal regulations. But help may soon be on the way. The Government Paperwork Elimination Act (GPEA), which was signed into law on Oct. 21, 1998, established a deadline of Oct. 21, 2003, to provide individuals or entities that deal with federeral government agencies the option to submit information or transact with the agency electronically and to maintain records electronically, when practicable. It also addresses the matter of private employers being able to use electronic means to store, and file with federal agencies, information pertaining to their employees.

Some areas of the USDA that should be greatly impacted by the move to electronic filing are the Farm Service Agency, the Risk Management Agency, Natural Resources Conservation Service and some rural development components of the USDA.

GPEA states that electronic records and their related electronic signatures are not to be denied legal effect, validity or enforceability merely because they are in electronic form. GPEA should be an important tool to improve customer

Don Rhodes is eStrategies policy manager with the American Bankers Association in Washington, D.C., and can be reached at (202) 663-7513.

service and governmental efficiency through use of information technology.

With the GPEA implementation date rapidly approaching, government agencies are moving quickly to address the challenges established by GPEA. The USDA recently contracted with a consulting firm to help develop a department-wide e-government plan.

How will a farmer or an agricultural lender be affected by GPEA? Why should you be interested in the technology known as Public Key Infrastructure (PKI)?

With the move to e-government, agencies will provide the means to file paperwork electronically, online and avoid those long lines at county offices. But to file that paperwork, or to interact with government agencies or business on the Internet, the agency or business involved will have to be sure that you are who you say you are – to guarantee your identity.

To successfully capitalize on the new opportunities of the Internet, companies, individuals and government must know their transactions are secure and must know with whom they are doing business. In other words, they must solve the problem of online identity. While GPEA is purposefully technology neutral regarding various electronic signature alternatives, it is apparent that one technology will emerge as the chosen alternative, in order to promote interoperability and ease of use.

While there are applications where personal identification numbers (PINs) and other shared secret techniques may be appropriate, there are applications where greater security is warranted. In these situations, cryptographically based digital signatures (i.e., public key technology) holds great promise for ensuring authentication and privacy in networked interactions, and may be the only technology that can foster interoperability across numerous applications.

What is an "electronic signature"? GPEA defines "electronic signature" as: "... a method of signing an electronic message that: a) identifies and authenticates a particular person as the source of the electronic message; and b) indicates such person's approval of the information contained in the electronic message." (GPEA, section 1709(1)).

An electronic signature could, in theory, be a click-through on a Web site, or a digitized version of a handwritten signature. An electronic signature could be a typewritten name. But these types of "electronic signatures" do not address the key elements of security on the Internet.

The four key elements of security on the Internet are:

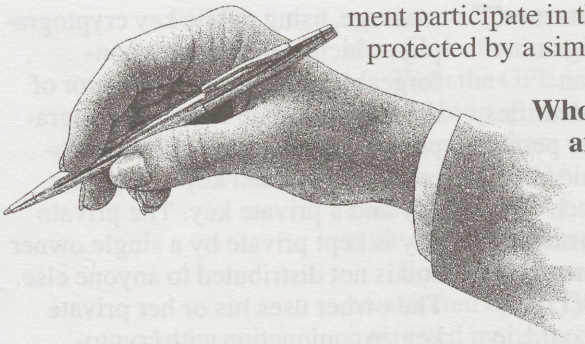
- *Authentication.* Is the person really who they say they are?
- *Data Integrity.* Has the message or transaction been altered during transit?
- *Non-repudiation.* Can either party falsely deny they took part in the transaction?
- *Confidentiality.* Can the message or transaction be intercepted and viewed by unauthorized parties?

While PINs, passwords and biometrics provide some level of authentication, they don't provide adequate solutions for all four elements of security. A digital signature, in conjunction with additional trust services and risk management infrastructure, not only provides authentication, but also guarantees message integrity, non-repudiation and confidentiality.

So what is a digital signature? It is a mathematical representation of a message, using public key cryptography, which identifies, in a non-forgeable manner, the originator of the message. Public key cryptography requires the use of two mathematically related keys – a public key and a private key. The private key is kept private by a single owner and is not distributed to anyone else. The owner uses his or her private key, in conjunction with cryptographic algorithms, to digitally sign a message. The public key is made public and can be used by anyone to verify the digital signature on a message. The fact that these two keys are mathematically related ensures that only a single private key can generate a digital signature that is verifiable by the corresponding public key, making the digital signature unforgeable.

The challenge now becomes binding a public/private key pair, in a reliable fashion, to an owner. This is where the digital certificate comes in. A digital certificate binds a person's identity to his or her public key, and, consequently, to his or her private key, and is used to verify digital signatures. Digital certificates and digital signatures then provide the foundation for secure e-business.

Although technology can provide this authentication, the real value of digital certificates comes from the policy and contract infrastructure backing it. This policy provides the framework for universally accepted digital certificates. The policy is analogous to the credit-card system foundation where a common rule set is in place that defines how merchants, banks, consumers or govern-



ment participate in the program. All parties are protected by a similar contract infrastructure.

Who are the parties involved and how do they relate?

Policy Management Authorities (PMA) develop, manage and implement the policy that governs the issuance of digital certificates. For the federal government, the General Services Administration (GSA) acts as the PMA for the government's Access Certificates for Electronic Services (ACES) Program. This program has established a Public Key Infrastructure to support digital signatures for government-wide use with the public. The PMA administers the policies and infrastructure of the ACES program to provide assurances that digital signatures are used appropriately and securely across government.

The ACES program is available to all federal agencies and currently a dozen federal agencies have signed on to use it. Next are Certification Authorities (CAs) which issue digital certificates and certificate revocation lists (CRLs). CAs usually are technology companies that actually issue the certificate under the guidelines as set by a PMA. Registration Authorities (RAs) identify certificate users. RAs could be banks, government agencies, employers or other entities willing to provide the due diligence necessary to meet stringent requirements for identification as required under certificate policies (CP) and to guarantee that identification through warranties. Repositories, publicly available databases, hold these certificates and certificate revocation lists, or provide for online status checking of certificates.

Using the credit-card system as an analogy, we can describe a potential digital certificate network. In this network, a certificate authority would be much like Visa or MasterCard. A registration authority would play the role of a

Visa or MasterCard issuing bank. The Policy Management Authority would govern the rule set which governs how certificates are used, what happens in instances where identification and authentication fails, or when certificates are misused. The PMA also governs the flow of insured risk and also the flow of fees to and from the involved parties, much as the rules of the credit-card associations provide this service to the card issuers, merchants and consumers.

The ABA, working with the Mortgage Bankers Association, has developed the TrustIDâ digital certificate program, which combines state-of-the-art technology with a sound policy and warranty program that guarantees identity in online transactions for the financial services industry. TrustIDâ is designed to serve both business-to-business as well as business-to-consumer needs. One of the most important questions when moving business processes online is "What happens if things go wrong?" This is where the TrustIDâ program stands alone. TrustIDâ digital certificates carry warranty protection that offers variable coverage up to $250,000 per certificate.

Digital Signature Trust Co. (DST), an affiliate of Zions Bancorporation and a partner with the ABA, was the first company awarded an "Access Certificates for Electronic Services" (ACES) contract by the General Services Administration (GSA). DST has received approval from the GSA on its digital certificate operations and can now issue ACES certificates to the American public on behalf of federal agencies. DST is the first ACES vendor to receive operational approval on its certificate issuance and repository services. DST also launched **www.ACESaccess.com**, an informational Web site designed to educate federal agencies on the benefits of the ACES contract and how to order contract services from DST and its ACES Team members.

DST was the first contractor awarded a three-year contract with a three-year option to issue digital certificates under the ACES contract. ACES certificates provide positive user identification in online transactions and enable federal agencies to fully use the Internet to improve service delivery and reduce overall costs. With ACES certificates, government agencies can provide more personalized services online, accept signed document filings online, and make working with the federal government faster and more convenient, in response to customer needs.

"The availability of ACES certificates marks the culmination of more than two years of development," says David Barram, GSA administrator. "This event represents another major milestone in our effort to provide the American people easy electronic access to government information."

"We are pleased to be a part of the enormous strides the U.S. government is taking to create services that are more accessible to Americans, more efficient and easy to use," says Keren Cummins, DST's vice president of government

services. "DST is excited to be GSA-approved and open for business to agencies who want to take advantage of the opportunities the ACES contract offers."

DST's ACES services accreditation came after successfully meeting the GSA's requirements and passing its rigorous operational and security tests. Under the ACES contract, DST has been providing consulting services to the National Institutes of Health since January 2000 when it won the first ACES task order. Receiving the GSA's accreditation is a green light for DST to actually issue digital certificates under ACES task orders from federal agencies. Through individual task orders with U.S. government agencies, DST creates customized online ACES "certificate centers," where agency employees, individuals and individuals acting on behalf of businesses can request ACES certificates.

For agencies looking for complete solutions, DST has assembled a "best of breed" ACES Team that translates into a comprehensive range of options to meet agency needs. DST Team members include Computer Sciences Corporation, BoozAllen·Hamilton, NCS, PricewaterhouseCoopers and others.

In addition to being the first selected and operationally approved ACES Certification Authority, DST is an approved CA for the U.S. Department of Defense Interim External Certificate Authority (IECA) PKI. DST also provides CA services to the states of California and Utah and to the electric utility industry's largest online trading community, OASIS.

So what does this mean to you on the farm or in the bank? It means that in the very near future, access to government should be easier, with streamlined service delivery back to you the citizen. It should reduce the burden on you and provide a fundamentally better customer experience. Access to government filings and information should be quicker, forms should be easier to fill out, faster to submit and should result in a more rapid response and processing

at the appropriate agency.

Government departments and agencies are working toward building common processes for digital signatures among agencies that serve common citizen and industry groups. Citizens and businesses will be able to use a single ACES certificate for digital signatures with multiple federal agencies for multiple purposes. For example, GSA has already organized four federal agencies (Education, Labor, Veterans Affairs and USPS) to commonly issue digital certificates to post-secondary students and schools. More than 100,000 ACES certificates are being issued to students and schools during the next two years for services in delivering student aid, filings to the government, and remote authentication. GSA has begun to organize the principal federal health-care agencies (Defense, HHS, Veterans Affairs) in conjunction with private industry efforts, to establish health-care PKI services that both industry and government can use. It is only a matter of time before USDA and affiliated agencies are included in the ACES program.

So will you, as an agricultural lender, need a digital certificate? The answer is not only yes, but a resounding yes! Digital certificates are in your future, as a consumer dealing with government and with online businesses. In the near future you won't ask what a digital certificate is. Instead, you'll wonder how we ever managed without them!

For more information, visit **www.digsigtrust.com.** **jal**