GOVERNMENT INSIGHT

Digital signatures transform California county's processes

By Rolf Bishop   May 18, 2016

Public sector paperwork is a problem in an increasingly paper-averse society. Forms sitting in folders inside of government offices, where people must come during work hours to fill out and sign -- or complete via mail or fax -- reflect arcane bureaucracies in the eyes of constituents.

Digital signatures, continued

Rightfully so. Paper processing handicaps back-office efficiency. Data entry adds steps, and even small amounts of time necessary for copying, scanning, printing and faxing add up and can tax a productive workday. (And who wants to wants to spend a lunch hour waiting in line at the county assessor's office to sign a form?)

After decades of relying on paper-based processes, the San Diego County's Assessor, Recorder and County Clerk's office, where I head IT operations, decided to pilot e-signing capabilities as a way to loosen paper's grip on our county. We deployed e-signatures for a single government process -- our residential change of address forms -- and in a matter of months began to see a return on our investment. We currently use digital signatures for four different county forms, and we save about $230,000 per year in ink, paper, storage and manual labor.

The process of finding the right e-signature technology that fit our needs for security and usability required due diligence and prioritization. First, we needed a hosted service so that our citizens could access and sign documents anywhere there is an Internet connection. The vendor also had to pass California's standards for acceptable digital signature providers.

Besides these criteria, there were three basic considerations to assess before choosing a software solution and presenting our e-signature pilot program to the public.

1. Perpetual validity

A government document is meaningless if it cannot be upheld in a court of law. So long-term e-signature validity was critically important when considering which technology would work best for our county.

Digital signatures, sometimes called independent e-signatures, are built on public key infrastructure (PKI), which uses public and private keys to show documents are indeed valid and unchanged. The legal evidence gathered through these keys is embedded permanently into a signed document, where it can be viewed by a PDF reader online or offline. That means digital documents will always be verifiable without relying on a specific vendor's solution and whether an Internet connection exists or not.

E-signatures that lack this PKI framework, by contrast, rely on proprietary technology to show legal evidence. A solution of that sort would lock our county into a vendor relationship and, since evidence is generally stored on a vendor's server and not embedded into a document, we would always need an Internet connection to prove validity.

SIGNiX THE MOST TRUSTED NAME IN DIGITAL SIGNATURES

www.signix.com | 877.890.5350 x1057 | sales@signix.com

2. Logging and securing the evidence

Consistent with our need for long-term legal evidence, a top priority was to have a comprehensive audit trail showing the signature's irrefutable provenance and integrity.

The audit trail must track every moment in the e-signing process, including document uploads, changes, identity authentication, document reviewing, initialing, etc. This would give us a firm timeline and narrative to support e-signature validity, should it ever be called into question. The technology must also alert users to any changes made to a document after any signature is applied -- further safeguarding the integrity of our forms and signatures.

3. Identity authentication

Public documents, by nature, must be safeguarded and signed only by the intended person. There are many different types of identity authentication methods we could choose from, including text message authentication, shared secret questions and the more detailed knowledge-based authentication -- which takes users through a rigorous series of questions pulled from information found in public databases.

In our case, we've found that email-only authentication -- which requires users to correctly input their email username and password -- meets our needs for online forms, as they generally do not contain sensitive personal information. However, should our needs expand to include higher-risk documents, we wanted a platform that could easily accommodate that change.

Freed from our paper bondage

Since we began using SIGNiX digital signatures in 2013, citizen satisfaction and operational efficiency have exceeded expectations. Consider that one of our processes -- the homeowner's exemption form -- was a 16-step manual process when it was paper-based. Now that it's online and signed with digital signatures, it's a simple two-step process that saves us tens of thousands of dollars annually. And our savings have multiplied as we've added this ability to other forms. The return on investment has been achieved in months -- not years -- and with assurance of validity and security, we will confidently expand our e-signature program in the future. ■

About the Author

Rolf Bishop is the CIO for the County of San Diego's Assessor, Recorder and County Clerk's office.