Shaking up your career path with a transition to, or within, higher education? To remain on course, apply the advice of university leaders who’ve been there.

Ground Control
When Digital Signatures Make a Debut at Colleges and Universities

In today's world, innovations emerge at a stunning rate and are often sparked by technology advances or capabilities. Such is the case with electronic and digital signatures, which have made their way into the business world and hold potential to make higher education processes more efficient as well.

However, as with many new procedures, business officers must view the adoption of digital signatures against the canvas of overall risk and the level of authentication required for specific transactions.

At this point, there is still debate in many universities about whether to accept digital signatures, continue the status quo of "wet ink" signatures, or develop hybrid signature methods. Digital signature transaction-management platform solutions can streamline and automate document signing, validate signed documents within business processes, and securely archive all signed documents to help accelerate transactions and reduce costs.

The University System of Alaska Fairbanks has been researching and piloting the use of digital signatures in several areas, including the offices of bursars, admissions, procurement, and finance—with transactions ranging from internal approvals, tuition waivers, memos, and approvals on routine business communications. With our recent experiences in mind, we’ll share some continued on page 6

Financial Aid FY12 Facts

- $6,500 Average amount of federal loans received by undergraduates receiving any federal aid in 2011–12.
- $8,200 Average amount of federal loans received by undergraduates receiving any federal aid in 2011–12.
- $10,000 Dependent students’ out-of-pocket net price by income in 2011–12.
- $13,800 Full-time, full-year dependent students’ out-of-pocket net price in 2011–12.
- $14,300 Average financial need among undergraduates with financial need, 2011–12.


www.nacubo.org
Digital Signature Implementation Stages

1. Strategy and sponsorship
   - Engage executive leadership.
   - Articulate the business case.
   - Outline behavioral changes.
   - Define success criteria.

2. Assessment
   - Motivate new behaviors.
   - Establish communication.
   - Identify and prioritize champions.
   - Listen to feedback.

3. Training
   - Identify your audience.
   - Map out a training schedule.
   - Deliver training.
   - Address user feedback.

4. Adoption
   - Maintain ongoing support.
   - Analyze user satisfaction.
   - Assess usage and adoption.

Source: University System of Alaska

The terms of a particular document, with the intent to sign. Under the Uniform Electronic Transactions Act, the signature is legally bound to the commitments made in the signed document. The electronic signature acts as an instrument of evidence regarding the authenticity of the electronic document in the same way as the handwritten signature does regarding paper-based documents. An important factor in the qualitative and quantitative estimation of the ways the system's current benefits align with institutional goals. The office of Information Technology coordinates the IT evaluation team, which includes representatives from various departments, and conducts the initial evaluation of the technology environment. Based on the results, strategic decisions are made regarding the areas suitable for pilot testing and implementation.

Organizational structure
- This assessment should include the nature of business processes in all functional areas, such as admissions, financial aid, human resources, facilities, athletics, and sponsored programs, that deal with financial transactions. There are areas where digital signatures can be easily implemented, such as employee time sheets, time sheet approvals, human resource forms, employee benefits, and specific activities and financial aid forms. However, the university policy needs to spell out clearly the business processes that can be conducted by digital signature approval methods.

Security policy
- The organizational security policy is mandated by various government regulations, including FERPA, HIPAA, Sarbanes-Oxley, and others. The university’s risk management, legal counsel, internal audit, information security, audit and records information management departments are pivotal in providing key inputs to the policy.

Strategy and Implementation Steps
- The institutions’ culture change cannot be achieved overnight. It is an effort to gauge support for the new signature process, it’s useful to change to benefits or changes in health plans.
- Before adopting a digital signature, it’s important to consider the university’s goals, as well as legal and audit compliance. The key factor to consider in implementing digital signatures is to identify the level of risk tolerance and the associated risk for a particular business process. In addition, university risks may involve financial, reputational, and other key administrative communications. Based on the various types of business processes and the level of severity, the assurance (which is a combination of authentication and validation) and trust levels have to be established. Functional area managers and organizations need to assess the level of risk, and to the extent to which one should secure the digital signature platform.

Digital signature rollout
- Based on the functional area needs for digital signatures, a quick assessment of the number of transactions and the level of approval required for a particular business process will provide a fairly accurate notion of the nature of the digital signature. For example, at most universities, the human resources benefits and health plan add/modifies forms require a "wet ink" signature on any particular business process to be provided.

The survey may include questions about the willingness of digital signature users. If a significant number of users are unwilling to sign documents digitally, it may be necessary to consider alternative solutions.

FAST FACT
- For many families, private loans are much cheaper than federal loans, which is a reason from every one year ago. — Wall Street Journal Blog, September 2014

Digital signatures, sometimes setting a threshold on the monetary value for financial transactions below which all approvals may be authorized by digital signatures. One way to pilot the plan is to conduct a phased implementation in low-risk functional areas in which transactions are monitored for proper usage, unauthorized access, and security breaches. With electronic transactions evolving at a rapid pace, digital signatures will become more acceptable. While the technology genie of digital signatures cannot be recaptured into the bottle, colleges and universities can balance the technology solution with the level of risk. "If you want to achieve the best solution for their processes and practices, you have to design a system that is more secure, efficient, and cost-effective."

SUBMITTED BY: Shiva Hallawarad, electronic content and electronic records administrator; Russell O’Hare, chief records officer; and Ashok Roy, vice president for finance and administration at the University of Alaska System. 

www.nacubo.org
considered four key steps (see figure for details).

A key factor to consider in implementing digital signatures is to identify the level of risk tolerance and the associated risk for a particular business process. In addition, University risks may involve financial, reputational, and other key administrative communications. Based on the various types of business processes and the level of severity, the assurance (which is a combination of authentication and validation) and trust levels have to be established. Functional area managers and organizations need to assess the level of risk, and to the extent to which one should secure the digital signature platform. This correlation poses a trade-off challenge to business managers and organizations willing to adopt digital signatures, thereby creating a dilemma to identify those business processes that require optimum levels of authentication and privacy.

Digital signature rollouts.
Based on the functional area needs for digital signatures, a quick assessment of the number of transactions and the level of approval(s) required for a particular business process will provide a fairly accurate notion of the nature of the digital signature. For example, at universities, the human resources benefits and health plan add/modifies forms require a "wet ink" signature on any particular business process is required to maintain employee information and benefits. This process can be streamlined by allowing the users to sign electronically and submit the signature to the appropriate department directly.

Digital signature implementation.
The institutions' culture change and the need for an efficient process can be just as important as the technical details. Before adopting a digital signature solution (or any other technology solution), we should be aware of the existence of the university's goals, as well as legal and audit compliance.

Key factors to consider in implementing digital signatures is to identify the level of risk tolerance and the associated risk for a particular business process. In addition, University risks may involve financial, reputational, and other key administrative communications.

The key to the success of the Digital Signature Implementation Initiative has been the establishment of a steering committee that includes representatives from various departments, and conducts the initial evaluation of the technology environment. Based on the results, strategic decisions are made regarding the areas suitable for pilot testing and implementation.

Organizational structure.
This assessment should include the nature of business processes in all functional areas, such as admissions, financial aid, human resources, facilities, athletics, and sponsored programs, that deal with financial transactions. There are areas where digital signatures can be easily implemented, such as employee timecards, timesheet approvals, human resources forms, employee benefits, and specific academic and financial aid forms. However, the university policy needs to spell out clearly the business processes that can be conducted by digital signature approval methods.

Security policy.
The organizational security policy is mandated by various government regulations, such as FERPA, HIPAA, Sarbanes-Oxley, and others. The university's risk management, legal counsel, internal audit, information security, and other organizational information management department are pivotal in providing key inputs to the policy.

Strategy and Implementation Steps.
The institutions' culture change and the need for an efficient process can be just as important as the technical details. Before adopting a digital signature solution (or any other technology solution), we should be aware of the existence of the university's goals, as well as legal and audit compliance.

A key factor to consider in implementing digital signatures is to identify the level of risk tolerance and the associated risk for a particular business process. In addition, University risks may involve financial, reputational, and other key administrative communications.