Digital Signature Feasibility Study

Final Report 534

Prepared by:

Arrowhead Solutions, Inc
16841 N. 31st Avenue
Suite 141
Phoenix, AZ 85053

June 2008

Prepared for:

Arizona Department of Transportation
206 South 17th Avenue
Phoenix, Arizona 85007

Technical Report Documentation Page

1. Report No. FHWA-AZ-08-534	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle **Digital Signature Feasibility Study**		5. Report Date June 2008 6. Performing Organization Code
7. Authors Chris Cioffi & Rob Fallows		8. Performing Organization Report No.
9. Performing Organization Name and Address Arrowhead Solutions, Inc 16841 N. 31st Avenue Suite 141 Phoenix, AZ 85053		10. Work Unit No. 11. Contract or Grant No. SPR-PL-1(59)534
12. Sponsoring Agency Name and Address Arizona Department of Transportation 206 S. 17th Avenue Phoenix, Arizona 85007 Project Manager: John Semmens		13.Type of Report & Period Covered FINAL 14. Sponsoring Agency Code

15. Supplementary Notes

Prepared in cooperation with the U.S. Department of Transportation, Federal Highway Administration

16. Abstract

The purpose of this study was to assess the advantages and disadvantages of using digital signatures to assist the Department in conducting business. The Department is evaluating the potential of performing more electronic transactions (e.g., electronic bidding, procurement, Motor Vehicle transactions, etc.) Many of the Department's candidate transactions require one or more ink signatures before they can be processed. The basic challenge is that without a means to provide verifiable and binding electronic signatures, many transactions become Internet ineligible and cannot become part of the Department's e-service portfolio. E-Government relies on secure communication between two or more trusting parties. Digital signatures may provide the missing component that would allow certain transactions to be performed electronically.

A great deal of information was found addressing digital signature technology and a number of case studies were used by the researchers. In addition, the researchers conducted a review of Arizona and Federal statutes to assess the legal requirements pertaining to the veracity of digital and electronic signatures. A survey of other states' transportation departments was completed to determine what digital signature technologies are being used. 36 states responded to the survey. Most states have either implemented a form of digital signature technology or are in the process of doing so. Most have chosen to leverage the capabilities of third-party software providers and not internal development by their staff. Finally, the researchers leveraged case studies and interviews with a leading digital certificate/PKI vendor to establish a basic cost profile for developing an internal solution and leveraging a third-party solution. The three year cost of a third party solution was significantly less than building a solution internally.

Based on the available sources, the researchers concluded that a well documented, third party electronic approval workflow application (e.g., AzDOT's use of Adobe's LiveCycle product) or a similar electronic approval workflow engine, provides the necessary structure to make virtually all internal processes and transactions compliant with Federal and State digital signature guidelines. It is important to note that a robust electronic approval process does not necessarily require the use of formal digital signature technology (e.g., Public/Private key digital certificates).

17. Key Words Digital Signatures, electronic signatures, electronic approval		18. Distribution statement		23. Registrant's Seal
19. Security Classification Unclassified	20. Security Classification Unclassified	21. No. of Pages 52	22. Price	

SI (MODERN METRIC) CONVERSION FACTORS*

APPROXIMATE CONVERSIONS TO SI UNITS

Symbol	When You Know	Multiply By	To Find	Symbol
	LENGTH			
in	inches	25.4	millimeters	mm
ft	feet	0.305	meters	m
yd	yards	0.914	meters	m
mi	miles	1.61	kilometers	km
	AREA			
in^2	square inches	645.2	square millimeters	mm^2
ft^2	square feet	0.093	square meters	m^2
yd^2	square yards	0.836	square meters	m^2
ac	acres	0.405	hectares	ha
mi^2	square miles	2.59	square kilometers	km^2
	VOLUME			
fl oz	fluid ounces	29.57	milliliters	mL
gal	gallons	3.785	liters	L
ft^3	cubic feet	0.028	cubic meters	m^3
yd^3	cubic yards	0.765	cubic meters	m^3
	NOTE: Volumes greater than 1000L shall be shown in m^3.			
	MASS			
oz	ounces	28.35	grams	g
lb	pounds	0.454	kilograms	kg
T	short tons (2000lb)	0.907	megagrams (or "metric ton")	mg (or "t")
	TEMPERATURE (exact)			
°F	Fahrenheit temperature	5(F-32)/9 or (F-32)/1.8	Celsius temperature	°C
	ILLUMINATION			
fc	foot candles	10.76	lux	lx
fl	foot-Lamberts	3.426	candela/m^2	cd/m^2
	FORCE AND PRESSURE OR STRESS			
lbf	poundforce	4.45	newtons	N
lbf/in^2	poundforce per square inch	6.89	kilopascals	kPa

APPROXIMATE CONVERSIONS FROM SI UNITS

Symbol	When You Know	Multiply By	To Find	Symbol
	LENGTH			
mm	millimeters	0.039	inches	in
m	meters	3.28	feet	ft
m	meters	1.09	yards	yd
km	kilometers	0.621	miles	mi
	AREA			
mm^2	Square millimeters	0.0016	square inches	in^2
m^2	Square meters	10.764	square feet	ft^2
m^2	Square meters	1.195	square yards	yd^2
ha	hectares	2.47	acres	ac
km^2	Square kilometers	0.386	square miles	mi^2
	VOLUME			
mL	milliliters	0.034	fluid ounces	fl oz
L	liters	0.264	gallons	gal
m^3	Cubic meters	35.315	cubic feet	ft^3
m^3	Cubic meters	1.308	cubic yards	yd^3
	MASS			
g	grams	0.035	ounces	oz
kg	kilograms	2.205	pounds	lb
mg	megagrams (or "metric ton")	1.102	short tons (2000lb)	T
	TEMPERATURE (exact)			
°C	Celsius temperature	1.8C + 32	Fahrenheit temperature	°F
	ILLUMINATION			
lx	lux	0.0929	foot-candles	fc
cd/m^2	candela/m^2	0.2919	foot-Lamberts	fl
	FORCE AND PRESSURE OR STRESS			
N	newtons	0.225	poundforce	lbf
kPa	kilopascals	0.145	poundforce per square inch	lbf/in^2

SI is the symbol for the International System of Units. Appropriate rounding should be made to comply with Section 4 of ASTM E380

Table of Contents

List of Tables

Glossary of Acronyms

AASHTO	American Association of State Highway and Transportation Officials
ABA	American Bar Association
AESI	Arizona Electronic Signature Infrastructure
AETA	Arizona Electronic Transactions Act
ANSI	American National Standards Institute
A.R.S.	Arizona Revised Statues
ASP	Application Service Provider
AzDOT	Arizona Department of Transportation
CAD	Computer Aided Design
ESI	Electronic Signature Infrastructure
FTE	Full-Time Equivalent
IT	Information Technology
KDOT	Kansas Department of Transportation
NECCC	National Electronic Commerce Coordinating Council
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
SLA	Service Level Agreement
SSO	Single Sign-On
TAC	Technical Advisory Committee
UETA	Uniform Electronic Transactions Act

Executive Summary

In March 2008 the Arizona Department of Transportation (AzDOT) initiated the Digital Signature Feasibility study. The purpose of this study was to assess the advantages and disadvantages of using digital signatures to assist the Department in conducting business. The Department is evaluating the potential of performing more electronic transactions (e.g., electronic bidding, procurement, Motor Vehicle transactions, etc.) Many of the Department's candidate transactions require one or more ink signatures before they can be processed. The basic challenge is that without a means to provide verifiable and binding electronic signage, many transactions become Internet ineligible and cannot become part of the Department's e-service portfolio. E-Government relies on secure communication between two or more trusting parties. Digital signatures may provide the missing component that would allow certain transactions to be performed electronically. They may also provide the desired level of security, privacy, and authenticity required for the Department's electronic messages. With the volume of e-commerce and business-to-business transactions increasing, the acceptance of digital signatures may be more a question of when, rather than if.

The project was divided into four major tasks:

- Interview Department staff whose work processes might be candidates for digital signatures.
- Review the literature on digital signatures and their legal veracity.
- Survey other state transportation departments to ascertain whether any use digital signatures.
- Develop advantages/disadvantages and cost/benefit profiles for digital signature usage by the Department.

What Is a Digital Signature and How DoesIt Work?

In the simplest usage of digital signatures, a user will sign an electronic document with his/her digital signature and then send the document to another person. The second person can electronically verify that the digital signature is valid and that the document has not been modified after it was signed. The second person will use digital keys, signatures and time stamps to enable "authentication" of electronic documents and assurance of the identity of the signature. The tools needed by both people in this process are provided by a Public Key Infrastructure (PKI) system and a trusted third-party certification authority. A PKI system creates and manages digital certificates. It is used to grant, renew, and revoke digital certificates for end-users. There are a number of standards for PKI messages; Arizona requires that PKI systems comply with American National Standards Institute (ANSI) x.509 and x.500 standards. To verify a signature, the verifier must have access to the signer's public key and have assurance that it corresponds to the signer's private key (which is always kept private). A trusted third party "Certification Authority" provides this service.

The main components of a Public Key Infrastructure (PKI) system include: digital signatures, public-key cryptography, certificate authorities, and enabling services. Public-key cryptography is the heart of a PKI system. It is a mathematical capability used to encrypt (secure) and decrypt (validate) using public and private keys. Digital signatures cannot be deployed without having a fully functional PKI system that is capable of generating and maintaining digital certificates.

Digital and Electronic Signature Legal Review

Arizona law sets forth specific requirements for electronic signatures that are used to "sign" documents filed with or by a state agency. A digital signature is a "type of electronic signature that transforms a message through the use of an asymmetric cryptosystem," (A.R.S. § 41-132(E) (3)). The Arizona Electronic Transactions Act (A.R.S. § 44-7001 et seq.) further demonstrates the legislature's concern with the veracity of electronic signatures in transactions relating to the conduct of business, commercial or governmental affairs.

State Agencies – A.R.S. § 41-132

Arizona law provides that an electronic signature "may be used to sign as writing on a document that is filed with or by a state agency, board or commission and the electronic signature has the same force and effect as a written signature," (A.R.S. § 41-132(A)). An electronic signature has to be (1) unique to the person using it, (2) capable of reliable verification, and (3) linked to a record in a manner so that if the record is changed the electronic signature is invalidated, (A.R.S. § 41-132(B)).

Arizona Electronic Transactions Act – A.R.S. § 44-7001 et seq. (the "AETA")

Arizona law recognizes that a record or signature in electronic form cannot be denied legal effect and enforceability solely because the record or signature is in electronic form, (A.R.S. § 44-7007(A)). Arizona law further recognizes that a contract formed by an electronic record cannot be denied legal effect and enforceability solely because an electronic record was used in its formation, (A.R.S. § 44-7007(B)). Arizona law also provides that an electronic record satisfies any law that requires a record to be in writing, (A.R.S. § 44-7007(C)). Finally, Arizona law provides that an electronic signature satisfies any law that requires a signature, (A.R.S. § 44-7007(D)). The AETA defines a secure electronic signature as one that is (1) unique to the person using it, (2) is capable of verification, (3) is under the sole control of the person using it, and (4) is linked to the electronic record so that if the record is changed the electronic signature is invalidated, (A.R.S. § 44-7031).

Retention Guidelines

According to Arizona and Federal guidelines, documents digitally or electronically signed are generally held to follow the same retention requirements as paper documents. Retention of digital signature documents is also addressed in the Signature Dynamics

Electronic Signing Policy for electronic signature usages created by the Policy Authority of the Office of the Secretary of State (April, 2002). The Electronic Signing Policy is intended for use by Arizona agencies, boards, commissions, and their electronic signing partners. It was created by the State of Arizona's Electronic Signature Infrastructure (AESI) and is managed by Arizona's Policy Authority.

In this policy document, under section 5.8.2 "Retention period for Archive" the signing process information must be retained for the "legal" life of the most enduring document signed within the ESI. If that "legal" life is unknown, then the information must be kept for at least 30 years. Specific record retention rule schedules for Arizona agencies are created and periodically revised by the Arizona State Library, Archives, and Public Records. The most recent revision was dated July 3, 2007, and contains specific guidelines Arizona agencies must follow for retaining documents related to all agency business functions.

Survey of other States' Department of Transportation

The researchers completed a survey of other states' transportation departments to determine how they are using digital signature technology. The survey started on April 17, 2008, and ended May 2, 2008. The researchers received responses from 36 states for a 75 percent response rate.

The objectives of the survey were to:

1. Understand use of digital signatures by other states' transportation departments and their plans to implement the technology in the future.
2. Determine which methods have been used to implement digital signature technology. Identify which software vendors were used and overall satisfaction with those vendors.
3. Understand how well transportation departments have achieved the benefits associated with their digital signature technology implementations (expectations, benefits, implementation challenges).

The use of digital signature technology is gaining traction with other states' transportation departments. More than half the respondents have already implemented the technology (55.6 percent). Of those that have not, 70.5 percent expect to do so within the next two to three years. Most transportation departments have chosen to leverage a third-party vendor for their digital signature implementations over building an internally hosted solution (88.9 percent use third-party software; only 11 percent have built an internal solution). The majority of states that have implemented digital signature technology report their programs have met or exceeded their expectations (72 percent). Not a single responding state believed its program wouldn't eventually meet expectations. The most commonly cited benefit to implementing digital signature technology was improved workflows and shorter times to obtain approvals on internal processes and procurement bids (named by 50 percent). Improved security/authentication was cited as a benefit by 23 percent and 23 percent said their primary benefit has been a reduction in printing and copying costs.

Cost/Benefit Profile of Digital Signature Technology Deployment at AzDOT

Another important aspect of the feasibility study was whether AzDOT should build a customized digital signature infrastructure internally or use a third-party solution. The researchers completed a high-level cost/benefit profile of the internal solution and one for a third party. From a cost perspective, the anticipated cost of developing an internal solution at an enterprise level has a three-year cost of $1,091,600 while leveraging a third-party solution had a three-year cost of $558,405.

Summary of Findings

Based on the available sources, the researchers concluded that a well-documented, third-party electronic approval workflow application (e.g., Adobe's LiveCycle or a similar electronic approval workflow engine) provides the necessary structure to make virtually all internal processes and transactions compliant with Federal and state electronic and digital signature guidelines. It is important to note that a robust electronic approval process does not necessarily require the use of formal digital signature technology (e.g., Public/Private key digital certificates).

Stakeholder Interview Section

The first task of the Digital Signature Feasibility study was to conduct interviews with key Arizona Department of Transportation stakeholders. The study's Technical Advisory Committee (TAC) provided a list of stakeholders who have been involved in previous digital signature research. All of the stakeholders interviewed were knowledgeable about the technology and were well acquainted with the history of digital signature research at AzDOT.

Table 1 – Summary of AzDOT Personnel Interviewed for the Study

Thomas Branham Sr. Manager	Account management for mainframe and distributed technologies. Responsible for security, firewall, intrusion, and anti-virus.
Giuly Caceres Sr. Project Manager	Project Manager in the Statewide Project Management Section.
Rich Nacinovich Manager	Server Team Leader responsible for application support, storage, backups, Exchange, and technical uplifts.
Daryl Odom Information Specialist IV	Supports infrastructure for the Engineering Technology Group. Responsible for archiving data, application support (CAD Apps), and researching new capabilities. Currently working on a digital signature proof-of-concept test.
Jamie Rybarczyk Information Technology Specialist	Technical support for firewalls, security, and digital driver's license support.
Suzan Tasvibi-Tanha Strategic Business Services Manager	Responsible for strategic technology planning, program management, program office functions, managing contractors, and liaison with consulting firms. Monitors legislation and supports many AzDOT special projects.

Interview Summary

The interviews provided background on the history of digital signature initiatives at AzDOT. In addition, they provided an opportunity for stakeholders to express input on how the technology would be best placed in the organization.

The researchers used a standardized interview guide to collect the following information:

Table 2 – Summary of Interview Results

Interview Objective	Result
Understand the background of digital signature work at AzDOT	The interviews oriented the researchers with several partially completed studies. Research on digital signatures at AzDOT dates back to 2002 and includes an actual technology pilot in 2004 that didn't move forward.
Collect previous documentation	The researchers were provided with documentation from the previous work.
Determine what the stakeholders are most interested in seeing in the feasibility study.	Results found on page 15
Understand the high-level cost of developing an in-house solution and determine if any cost analysis is available.	Between 2002 and 2004, AzDOT staff worked on a Project Investment Justification document that contained helpful "cost" information. This information is considered further in the study.
Identify transactions/processes that are candidates for digital signatures	Results found on page 16
Understand the stakeholders' perspective on benefits / concerns of deploying digital signature technology	Results found on pages 17-18

Stakeholder's Expectations of Digital Signature Feasibility Study Outcomes

In addition to the deliverables stated in the feasibility study statement of work, each stakeholder was asked what were the most important items he would need to see in the final report. The following expectations were expressed by these stakeholders:

1. Recommendations for "building" versus "buying" a digital signature solution.
2. A summary of other states' efforts relative to digital signatures and how AzDOT compares.
3. A perspective of the lessons learned by the other states.
4. A summary of Arizona state government's efforts relative to digital signatures and how AzDOT compares.
5. Document the legal veracity of digital signatures and retention requirements.
6. Clearer direction on the path AzDOT should be taking with digital signature technology.

Candidate Transactions Identified

Each stakeholder was asked to identify potential transactions that might be candidates for digital signature technology. Nearly all stakeholders mentioned the first three transactions listed below. Some have only internal impacts, though a few that also have external impacts.

Candidate transactions:	Impact:
1. Engineering documents / Plan drawings	Internal / External Vendors
2. AzDOT employee system access requests	Internal impact only
3. Employee timesheets	Internal impact only
4. Interaction with law enforcement (DMV)	Internal and external impact
5. Project files	Internal impact only
6. Training requests	Internal impact only
7. Motor vehicle registrations customers	Internal and external

Potential Benefits of Digital Signature Technology from the Stakeholder's Perspective

The stakeholders interviewed said they supported the idea of implementing some form of digital signature technology. A number of potential benefits were mentioned; however, these benefits have not been quantified or proven. The engineering team articulated a strong potential business case and is quantifying the possible savings. At this point, based on these interviewee comments, the possible, but as yet unproven, benefits include the following:

- Process flow improvements for documents requiring multiple "approvals"
- Speeding of the approval process
- Reduced costs
- Data storage improvements
- Improved disaster recovery over paper archiving
- Improved retrieval process
- Alignment with Arizona and Federal E-Sign and electronic signature directives
- Improved readiness for new legislation

The business case for digital signature technology for Engineering:
The most compelling business case was made by the Engineering team. Although it has not quantified the benefits yet, it is in the process of putting the analysis together. The primary benefits mentioned were:

- Reduction in printing and paper costs associated with designs/drawings for large-scale projects. Because the Engineering Technology Group uses highly specialized, large-sheet printers, the cost savings could be substantial,
- Improved data storage and retrieval processing,
- Reduction in legal risks associated with misplacing signed documents in paper archives,
- Reduced cost through more efficient electronic workflow for plan drawing processing.

Stakeholder Concerns about Digital Signature Technology

Table 3 – Summary of Stakeholders' Concerns

Concerns	Commentary
Solution must be end-to-end	The stakeholders understand that implementing digital signatures means much more than just the technology behind digital certificates. The solution must have a complete and well-documented workflow and robust change management/training process.
Avoid implementing in a silo	The stakeholders recognized the changes required to successfully implement digital signatures go well beyond the direct control and purview of IT.
Impact of pending legislation	New legislation was enacted by the state legislature that will mandate electronic processing of transactions such as vehicle registration. The stakeholders are very concerned about the readiness for this change and the aggressive dates requireded in the legislation.

Review of Existing Literature

The second task of the Arizona Department of Transportation Digital Signature Feasibility Study required the researchers to review existing literature on the topic of digital signatures. The review included documentation from many different sources:

- Arizona Statutes, Administrative Codes, and policy documents,
- Federal statutes, policies, and white papers,
- Independent research compiled from documented case studies, vendor products, and other sources,
- Existing SPR-534 project archives.

The information from these sources was used to create this document.

Documents Reviewed During Feasibility Research

State of Arizona Statutes, Administrative Codes, and Policy

Table 4 – Arizona Statutes, Administrative Codes, and Policies

Document	Summary
A.R.S. 41-132 – Electronic and digital signatures: exemptions; definitions	Provides that electronic signatures have the same force as a written signature.
A.R.S. 41-1351 – Determination of Value; Disposition	Assigns responsibility for setting document retention rules to the Arizona State Library, Archives, and Public Records.
A.R.S. 44-7001 – Arizona Electronic Transactions Act	Recognizes that a record or signature in electronic form cannot be denied legal effect and enforceability solely because the record or signature is in electronic form
A.R.S. 44-7012 – Electronic records retention; originals	If the law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record.
A.R.S. 41-121 Duties of the Secretary of State	Provides authority to the Secretary of State to establish policies and procedures for the use of electronic and digital signatures by all state agencies, boards, and commissions.
Session Laws, Forty-eighth Legislature, Second Regular Session, 2008, Chapter 177: Vehicle title; registration; electronic signatures	Legislation passed in 2008 relating to electronic vehicle title and registration
Arizona Administrative Codes: Chapter 12. Office of the Secretary of State, Article 5. Electronic Signatures	Establishes specific requirements for and definitions of electronic signature technology and the role the Secretary of State's office has for approving all technologies relating to electronic signatures.

Document	Summary
Signature Dynamics Electronic Signing Policy for electronic signature use. State of Arizona, Policy Authority, Office of the Secretary of State. Arizona Electronic Signature Infrastructure (AESI) April 2002	Overview of Electronic Signing Policy intended for use by State of Arizona agencies, boards, and commissions and their electronic signing partners. Policy outlines business process scope, technical requirements, technical security controls, and establishes levels of trust.
Policy Authority Procedure for the Arizona Electronic Signature Infrastructure (AESI) September, 1999	The Policy Authority is responsible for defining and managing the Arizona Electronic Signature Infrastructure (AESI). The AESI consists of all of the State of Arizona's collections of electronic signing mechanisms and the entities and tools that enable the valid use of these forms of signatures.
Policy Authority Procedures for the Arizona Electronic Signature Infrastructure (AESI) April 25, 2002	Policy update that provides requirements for PKI, PGP, and other elements of Signature Dynamics Electronic Signing Policy.
Arizona State Library, Archives, and Public Records General Records Retention Schedule for All State Agencies – Schedule Number 000-07-41 July 3, 2007	Pursuant to ARS 41-1351, document contains both the minimum and maximum time records may be kept by Arizona agencies.
Records Retention and Disposition for Arizona State Agencies Arizona State Library, Archives, and Public Records Management Division; March, 2002	Discusses the life cycle of records and outlines retention rules for all different types of state transactions and documents.

Federal Government – E-Sign Documentation

Table 5: Federal Government E-Sign Documents

Document	Summary
NECCC E-Sign – An introduction to E-Sign Interoperability Workgroup and State Electronic Records and Signatures Reciprocity and Inter-operability Issues. December 2001	This work group established guidelines used by the Federal and state governments to define the essential requirements for a formally formed electronic record and signature. Established rules that helped guarantee that a signed document has legal effect, both for sender and receiver, within each state and beyond its borders.
Framework for Electronic Signature Reciprocity (part of E-Sign) E-Sign Interoperability Work Group – White Paper December 2001	Provides objective criteria for determining levels of trust in electronic signatures and e-records.
Record Retention Analysis Under E-Sign National Electronic Commerce Coordinating Council – White Paper December, 2001	E-Sign established on June 30, 2000, when President Clinton signed the Electronic Signatures in Global and National Commerce Act. This white paper allows state regulatory agencies to set performance standards for electronic records that law, rules, or regulations require private entities to retain. It was written to explain E-Sign's impact on the authority of states to require that private parties retain written records of certain transactions.
Electronic Records Management Guidelines for State Governments. (Part of E-Sign) Ensuring the Security, Authenticity, Integrity, and Accessibility of Electronic Records. National Electronic Commerce Coordinating Council – White Paper December 2001	Established practical guidelines to help agencies develop effective electronic records management procedures. The guidelines provide a general direction on how state government agencies can ensure the authenticity, integrity, security, and accessibility of electronic records.
Signature Dynamics Electronic Signing Policy for electronic signature use. (Part of E-Sign) State of Arizona, Policy Authority, Office of the Secretary of State. Arizona Electronic Signature Infrastructure (AESI) April 2002	Overview of Electronic Signing Policy intended for use by State of Arizona agencies, boards, and commissions and their electronic signing partners. Policy outlines specifics including business process scope, technical requirements, technical security controls; and establishes levels of trust.

Document	Summary
Impact of Electronic Signatures on Security Practices for Electronic Documents (Part of E-Sign) A National Electronic Commerce Coordinating Council White Paper; December 2001	Discusses the challenges of maintaining public records integrity under E-Sign and UETA. It introduces a document classification scheme, a best practice state governments can adopt, and helps them face the security challenges of E-Sign.

Independent Research – Vendor White Papers, Case Studies, and Miscellaneous Research

Table 6: White Papers and Case Studies

Document	Summary
VeriSign Adobe Certified Document Services – Enterprise signing – enterprise true credentials Adobe Acrobat from VeriSign product materials No date included	Overview of VeriSign document services and digital signature solutions/tools.
Electronic Document Security: A Guide to Certified Digital Signatures VeriSign; White Paper No date included	Included an overview of digital signature technology (including PKI), legal issues, Adobe products, and several case studies (Penn State Univ., Orexigen Theraputics, Inc).
4 Point Solutions Product Overview No date included	Overview of 4 Point Consulting offerings with Adobe. This consulting company is being used by the IDE group for their current Digital Signature Pilot.
"KDOT Shifts Into High Gear" Silanis Technologies No date included	Case study of the Kansas DOT adoption of electronic forms, workflow, document management, and electronic signatures
"Kentucky's Department of Natural Resources" Silanis Technologies No date included	The Department's move towards a paperless environment. Completing the circle of information for real-time, status update on mining projects.
ARX – Algorithmic Research White Paper on the CoSign Digital Signature Technology solution No date included	Overview of business benefits, features, legal compliance, and technical requirements of digital signatures. Discusses the use of Portable Document Format (PDF) and Acrobat.

Document	Summary
American Bar Association – Digital Signature Guidelines Tutorial No Date Included	An overview published by the ABA on digital signature technology, the law, and the challenges associated with implementing this technology.
"Digital Signature Guidelines" American Bar Association August 1, 1996	An early set of guidelines and the law covering the use of digital signature technology.
Oregon Department of Transportation – Digital Signatures for Engineering Documents June 25, 2007	Outlines issues relating to the utilization of digital signatures on engineering related documents with the Oregon Department of Transportation.
"Public Key Infrastructure Q&A" Gartner Group Report November 13, 2002	Public key infrastructure security has failed to achieve widespread adoption, mostly because enterprises rarely need all of its benefits.
"Time's Running Out to Prove the Value of Government PKI" Gartner Group Report October 27, 2004	Discusses the difficulties many Federal and state agencies have encountered when attempting to implement PKI technology.
"Apply the Lessons of Public-Key Infrastructure (PKI) to Protecting Customer Information" Gartner Group Report March 25, 2005	The basic concepts underlying PKI are applicable to most challenges encountered in protecting customer information.
"Management Update: Apply the Lessons of Public-Key Infrastructure to Protecting Customer Information" Gartner Group Report April 6, 2005	How PKI concepts can be applied to protect customer information.

Review of Previous AzDOT Digital Signature Technology Research

Table 7: Previous AzDOT Research

Document	Summary
Project Investment Justification – SPR-534 Digital Signatures Written by: David Moy, ITG, AzDOT Multiple versions: 11/30/2004, 3/272002	Developed by AzDOT ITG to justify a pilot implementation of PKI technology.
AzDOT Information Technology Group – SPR 534: Digital Signature Feasibility Study May 18, 2004	A partial report summarizing the results of a previous feasibility study effort in 2004.
AzDOT Uses for Digital Signatures – Phase 1: Pre-pilot Report 534 March, 2002	Report outlines the impact that digital signatures and electronic forms can have on AzDOT. Emphasizes the importance placed on AzDOT becoming its own Certificate Authority and managing the entire system internally.

Digital Signature Definition – What is PKI?

Two documents that are included in the project archives for SPR 534 – Digital Signatures Project provide an excellent definition and overview of Public Key Infrastructure (PKI):

- Oregon Department of Transportation. *Digital Signatures for Engineering Documents*. June 2007.
- Arizona Department of Transportation. *SPR 534: Digital Signatures – Feasibility Study*. May 2004.

A summary (with edits) of the definitions these documents provide is as follows:

Traditional hand written, or "wet," signatures on physical documents worked well during the era of hand written/drawn documents. A wet signature's purpose is not to prove identity, but rather to show agreement or consent. We" signatures are not always binding unless witnessed. The tasks for creating drawings and documents have been moved to computers to increase productivity and accuracy in nearly all facets of business within AzDOT. Electronic documents are routinely transmitted in bidding processes and amongst internal units. Management, storage, and retrieval of these documents with wet signatures have become increasingly problematic. Signed documents that are physically stored require a great deal of space and are often difficult to track and recall. Documents that are signed and scanned and then stored again electronically lose the original document electronic format; scanning is also a time consuming process. Digital Signatures can be used to speed workflow, support repudiation processes and can significantly help support sound document management practices.

In the simplest usage of digital signatures, a user will sign an electronic document with his/her digital signature and then send the document to another person. The second person can electronically verify that the digital signature is valid and that the document has not been modified after it was signed. The second person will use digital keys, signatures, and time stamps to enable "authentication" of electronic documents and assurance of the identity of the signature. The tools needed by both people in this process are provided by a Public Key Infrastructure (PKI) system and a trusted third-party certification authority.

- A PKI system creates and manages digital certificates. It is used to grant, renew, and revoke digital certificates for end-users.
- A PKI system can be used to manage both public and private keys.
- There are a number of standards for PKI messages; Arizona requires that PKI systems comply with ANSI x.509 and x.500 standards.
- In order to verify a signature, the verifier must have access to the signer's public key and have assurance that it corresponds to the signer's private key (which is always kept private). A trusted third party Certification Authority provides this service.

The main components of a Public Key Infrastructure (PKI) system include: digital signatures, public-key cryptography, certificate authorities, and enabling services.

Public-key cryptography is the heart of a PKI system. It is a mathematical capability used to encrypt (secure) and decrypt (validate) using public and private keys. Digital Signatures are specially designed with public-key cryptology so that they can provide:

1. Authentication: the ability to verify the identity of a user or an organization.
2. Integrity: protection against unauthorized modification or substitution of information in a document, transaction or other type of message.
3. Privacy: security against eavesdropping or interception of private data.
4. Non-repudiation: absolute certainty that a specific digital certificate was used to sign a document, transaction or other type of message.

Using the capabilities of digital certificates, PKI systems can be used in many facets of electronic services, including (but not limited to):

1. Digital Certificates that can be used to electronically sign or authorize contracts, purchase orders, engineering documents, documents, and critical e-mail.
2. Logon and Single Sign-on (SSO) that enable users to maintain a user id and password which grants them a right to use system resources and access data.
3. Electronic Commerce transactions that prove to the seller and the bank that the purchaser is who he says he is to assure a proper funding authorization.

Digital Signatures cannot be deployed without a having a fully functional PKI System that is capable of generating and maintaining digital certificates. With this technology in place, AzDOT would be able to:

1. Electronically authenticate the identity of internal staff and external service providers or consumers,
2. Protect the integrity of sensitive and confidential data,
3. Realize benefits of improved workflow (less paper handling, improved responsiveness, reduced research time),
4. Enforce non-repudiation issues that occur as a result of e-business transactions.

Digital Signature Implementation Approaches

There are three general approaches that AzDOT has explored and considered to implement digital signature capabilities. These general solutions are: 1) a customized internal solution, 2) an internally hosted packaged solution, and 3) an externally hosted (or Application Service Provider- ASP) solution.

Customized Internal Solution

Florida created an internally customized PKI System and Certificate Authority. This has been ruled out as an option for AzDOT due to the degree of scientific complexity, the staff resources that would be required, probable delays and integration with other queued projects, and the need to form a management department to support signature authentication.

Internally Hosted – Packaged Solution

In this approach, AzDOT would select a vendor-packaged PKI System and implement it on servers within the state government's computing infrastructure. Over a period of time, and as need arises, existing applications would be modified to use the PKI System services. A third-party vendor would be selected to act as a "trusted certificate authority" to validate signatures.

This solution is viewed as being the best because it has the benefit of leveraging existing market functionality and expertise with minimal impact to AzDOT resources and projects. Integration could begin with the highest priority needs as soon as the hardware and software were in place and the support staff could be trained. AzDOT would be positioned to manage ongoing maintenance releases directly and could coordinate with other applications maintenance and release opportunity windows.

Externally Hosted Solution

Application Service Providers, (ASPs) offer software hosted on their hardware. Clients, in this case AzDOT, would link to the ASP over telecommunications circuits to perform PKI system management functions. Although an ASP solution would create an opportunity to immediately begin issuing digital certificates, the solution is not viewed as being plausible.

Hosting confidential data such as public and private keys offsite is a significant security risk. Creating extensive dependence on an outside provider is viewed as being problematic to manage as the services would be required to be placed for bid periodically, thus potentially creating unnecessary work to train, convert, and transition staff as well as systems testing and integration activities to use other providers. Finally, this approach would make ongoing integration with internal systems more difficult and expensive.

Commonly Cited Benefits of an End-to-End Digital Signature Process

Table 8: Commonly Cited Benefits of Digital Signatures

Benefit	Description
Reduction in printing costs	Documents available to sign electronically and easily re-distributed without need to reprint. Especially important for the AzDOT Engineering group where specialty paper/printing is used. In addition, there are high volumes of printing during the bid process.
Reduction in administrative costs	Reduction in costs associated with copying, filing, and faxing documents. Reduction in time spent tracking down approvals.
Elimination of scanning expenses	Many companies/agencies use internal staff and/or third-party outsourcing to convert paper documents into scanned images.
Streamlined processes by automating routing of approvals	Significant cost reduction and improved turnaround times for approvals. Case studies showed average reduction of 60 percent-80 percent in the turnaround time required to get documents approved, when completed electronically versus by mail.
Improved disaster recovery	Unlike paper archives, if set up properly, electronic documents can easily be accounted for in disaster recovery plans.
Improved security	For even the most secure transactions (Federal government top secret ratings) PKI technology has been proven to be more secure than any previous technology.
Expand access to valid users; restrict access for users that do not have authority	Because information is available electronically and users can be authenticated using digital signature technology, simpler and more secure access can be granted.
Repudiation	"Wet" signatures are not reputable unless witnessed. Digital signatures are completely binding.

Digital Signatures – Part of an End-to-End Document Life Cycle

Much has been written about the underlying technology involved in digital signatures. Often, too much emphasis is placed on the technology itself and not enough on how digital signatures fit within the larger end-to-end view of the document life cycle. Even the partially implemented ITG PKI solution focused primarily on the digital certificate technology with minor, if any, focus on how the technology should be integrated into an end-to-end workflow.

The following processes must be considered within the scope of an end-to-end digital signature process:

1. Electronic Forms Library: Creating a central place where customers can access online forms optimized by an end-to-end solution. Usually developed as part of an intranet portal used by the department.
2. Workflow Management / Electronic Approvals: Implementing a workflow tool to manage electronic approval flows. This form of workflow tool may or may not include PKI technology. Most implementations do not according to the cases we reviewed.
3. Document Imaging: The process of converting paper forms for electronic storage is an important aspect of any solution.
4. Document Management: How documents are stored and managed once approved. This includes the establishment of retention rules for each document type.
5. Document Archiving and Retrieval: The process used to quickly access documents. Must have robust search capabilities along with a proper level of security to ensure that only authorized users can access the archived documents.

Commonly Cited Implementation Challenges

Table 9: Commonly Cited Implementation Challenges

Limited Participation	Need to include all affected departments early in the project including: • IT (Infrastructure & application) • Business Process Owners: those individuals knowledgeable about the process being automated • Security / Risk Management • Management • Legal • Training
Poor Deployment Planning	Not communicating with affected groups, not implementing the necessary training, and not gaining customer input on high-value processes to automate. Lack of post-implementation support.
Lack of Formal Training / Change Management Planning	Many implementations suffer due to lack of a thorough training plan.
Requirements Not Well Documented	Not getting the end-to-end process chain ready. Each process and electronic document needs to be thoroughly analyzed.
Not Recognizing Long-Term Rollout Approach	Moving to a digital signature process is a long-term transformation, often requiring years to fully realize the benefits. Even in the most well-documented case study, that of the Kansas DOT, it has taken 5+ years to implement digital signatures, with investments likely in the millions of dollars.
High Costs / Complicated Integration	Cost of implementing digital signatures goes beyond the initial investment in technology infrastructure and digital signature software technology. It involves investments in creating form libraries, improving imaging capabilities, developing new document management solutions, etc.
Poor User Adoption Rates	Customers may not understand the new processes, or were not consulted about what transactions/processes should be automated to benefit them the most. It is also very important that the solution developers balance security with ease of use. Too much security at the expense of ease of use leads to poor adoption rates.
Management Pitfalls	Lack of executive sponsorship necessary to set the project as multi-year and high priority. Not securing buy-in from business, no or late customer involvement (this cannot be an “IT only” project), and not setting proper expectations about the long-term nature of this project.

Digital Signature Technology Legal Review

Prior to implementing a digital signature technology solution, it is important to understand the legal consequences of using this method of conducting business. The following section looks at several aspects of the digital signature process:

1. What is Arizona law regarding the use of electronic/digital signatures?
2. What is the veracity of electronic signatures?
3. What are the specific retention requirements for electronic documents?

What is Arizona law regarding the use of digital and electronic signatures?

Brief Answer

Arizona law sets forth specific requirements for electronic signatures that are used to "sign" documents filed with or by a state agency. Arizona law also sets forth very specific requirements for documents that are "signed" by a digital signature, a type of electronic signature. Second, the Arizona Electronic Transactions Act further demonstrates the concern of the legislature with the veracity of electronic signatures in transactions relating to the conduct of business, commercial or governmental affairs. Finally, there has been only one challenge to electronic signatures in Arizona, and it was unsuccessful.

Discussion

I. State Agencies – A.R.S. § 41-132

Arizona law provides that an electronic signature "may be used to sign as writing on a document that is filed with or by a state agency, board, or commission, and the electronic signature has the same force and effect as a written signature" (A.R.S. § 41-132(A)).

An electronic signature is "an electronic or digital method of identification that is executed or adopted by a person with the intent to be bound by or to authenticate a record" (A.R.S. § 41-132(E) (4)).

An electronic signature has to be (1) unique to the person using it, (2) capable of reliable verification, and (3) linked to a record in a manner so that if the record is changed the electronic signature is invalidated (A.R.S. § 41-132(B)).

A document that has an electronic signature that is a digital signature has to comply with additional specific requirements.

A digital signature is a "type of electronic signature that transforms a message through the use of an asymmetric cryptosystem" (A.R.S. § 41-132(E) (3)).

An asymmetric cryptosystem is defined as "an algorithm or series of algorithms that provide a secure key pair for a digital signature" (A.R.S. § 41-132(E) (1)).

The requirements of a document containing a digital signature are:

(a) The document must contain a computer-based certificate that
  (1) identifies the issuing entity and the subscriber (the subscriber lawfully holds the private key that corresponds to the public key listed in the certificate and accepts the certificate),
  (2) contains the subscriber's public key, and
  (3) is digitally signed by the issuing entity.
    (i) An issuing entity is "a person who creates and issues a certificate and notifies the subscriber listed in the certificate of the contents of the certificate" (A.R.S. § 41-132(E)(5)).

(b) The document must contain a key pair used for verifying a digital signature that has a unique property so that the public key can verify the digital signature that the private key creates.
  (i) A key pair is "a private key and its corresponding public key in an asymmetric cryptosystem." (A.R.S. § 41-132(E)(6)).

(c) The document must be capable of verification by the person having the initial message and the signer's public key, meaning that
  (1) the person can accurately determine whether the transformation of the message was created by using the private key that corresponds to the signer's key and
  (2) the person can accurately determine whether the initial message has been altered since the transformation was made.
    (i) Transform means to "subject data in a message to a mathematical change by electronic means" (A.R.S. § 41-132(E)(12)).

The legislative history of A.R.S. § 41-132 shows that the statute was intended to define the necessary terms regarding electronic signatures to allow the Arizona Secretary of State to adopt rules regarding electronic signatures.

II. Arizona Electronic Transactions Act – A.R.S. § 44-7001 et seq. (the "AETA")

Arizona law recognizes that a record or signature in electronic form cannot be denied legal effect and enforceability solely because the record or signature is in electronic form (A.R.S. § 44-7007(A)). Arizona law further recognizes that a contract formed by an electronic record cannot be denied legal effect and enforceability solely because an electronic record was used in its formation (A.R.S. § 44-7007(B)). Arizona law also provides that an electronic record satisfies any law that requires a record to be in writing (A.R.S. § 44-7007(C)). Finally, Arizona law provides that an electronic signature satisfies any law that requires a signature (A.R.S. § 44-7007(D)).

The AETA defines a secure electronic signature as one that is (1) unique to the person using it, (2) is capable of verification, (3) is under the sole control of the person using it, and (4) is linked to the electronic record so that, if the record is changed, the electronic signature is invalidated (A.R.S. § 44-7031).

The legislative history of the AETA shows that it is modeled after the Uniform Electronic Transactions Act (UETA) and was meant to address concerns regarding the incompatible laws between states and the use of electronic signatures by private parties in business transactions. The AETA applies to parties that elect to conduct electronic transactions or to form electronic contracts using electronic signatures.

III. Challenges to Electronic Signatures in Arizona

Case law on challenges to the veracity of electronic signatures in Arizona is virtually non-existent. One recent case has upheld the veracity of electronic signatures in the judicial arena. In that case, plaintiffs challenged the validity of two electronic signatures by the superior court judge on two separate judgments. *Haywood Sec., Inc. v. Ehrlich*, 214 Ariz. 114, 115, ¶ 3, 149 P.3d 738, 739 (2007). Plaintiffs argued that the electronic signatures on the judgments did not satisfy the "signed" requirement of Rule 58(a), *Arizona Rules of Civil Procedure*, which requires that all judgments be in writing and signed by the judge. *Id*. at ¶ 2. The Arizona Supreme Court, sitting *en banc*, held that the judge's electronic signature on the judgments "clearly demonstrated his intent to authenticate both documents, and [he] therefore 'signed' them for purposes of Rule 58(a)." *Id*. at 117, ¶ 15, 149 P.3d at 741. The Court went on to state that its holding comports with the AETA's "general policy of recognizing and facilitating transactions using electronic signatures." *Id*. at 117, n.2, 149 P.3d at 741.

There have been no legal challenges to A.R.S. § 41-132.

IV. Challenges to Electronic Signatures in Other Jurisdictions

It appears that many states have also adopted the UETA or some version of the UETA. There is limited case law in other jurisdictions discussing the veracity of electronic signatures.

Electronic signatures have been held to satisfy the Statute of Frauds. In one case, the parties had entered into an agreement regarding the sale of goods through a series of e-mails. *Int'l Casings Group, Inc. v. Premium Standard Farms, Inc.*, 358 F.Supp.2d 863, 865 (W.D. Mo. 2005). The seller, in an attempt to back out of the contract, argued that the Statute of Frauds prevented enforcement of the contract for the sale of goods because the contract was not in writing and was not signed. *Id*. at 872. The United States District Court for the Western District of Missouri held, citing to Missouri law that had adopted the UETA, that even though the parties' signatures were electronic, it satisfied the Statute of Frauds as long as there was an intention to authenticate the documents. *Id*. at 873. The Court noted that its finding that an electronic signature in an email satisfied the Statute of Frauds is supported by developing case law. *Id*. at 874.

Just because an electronic signature has the same effect by law as a hand-written signature does not preclude a person from arguing that he did not authorize the electronic signature. In one case, the appellant argued that the bankruptcy court incorrectly disregarded a document filed by the appellee with the Securities and Exchange Commission that bore an electronic signature. *Piranha, Inc. v. Piranha, Inc*., 297 B.R. 78, 81 (N.D. Tex. 2003) The United States District Court for the Northern District of Texas held that Delaware law, that had adopted the UETA, did not advocate the enforcement of electronic signatures that were neither executed, adopted, nor authorized. *Id*. at 82. Citing a section of the UETA that provides that an "electronic signature is attributable to a person if it was the act of the person," the Court held that UETA does not preclude a person from contesting that he executed, adopted, or authorized an electronic signature that is purportedly his.

Document Retention Guidelines

What are the policies governing the retention of electronic documents?

The legality of an electronically signed record requires that it "remains accessible to all persons who are entitled to access by statue, regulation, or rule of law, for the period required by such statute, regulation, or rule of law, in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing or otherwise." [1]

According to State and Federal guidelines, documents digitally or electronically signed are generally held to follow the same retention requirements as paper documents.

> "Government's record retention, whether paper or electronic, is intended to give evidence of some action. E-sign policy establishes that record retention requirements of electronic records created by electronic signatures are not different than retention requirements for paper records."[2]

However, Section 101 (d) (1) of the E-Sign Act further qualifies this general rule. It provides that where a statute, regulation, or rule of law requires that a contract or record in a transaction in or affecting interstate or foreign commerce be retained, an electronic record only meets the statutory requirement if:

1. The record is accurate,
2. The record is accessible in a form that can be accurately reproduced; and
3. The record is accessible to all persons entitled to review the record.

[1] Federal Electronic Signatures in Global and National Commerce Act, Section 101. (d)(1)(B) (E-Sign- Interstate and international commerce)

[2] National Electronic Commerce Coordinating Council (NECCC) "Impact of Electronic Signatures on Security Practices for Electronic Documents." (December, 2001)

Guidelines Established by the NECCC E-Sign Workgroup

Just as with paper records, the e-records a government agency produces or receives are not all of equal importance or value. Although all government records should be maintained properly, the effort and resources a state agency expends to manage and maintain records, including e-records, should be related to the records' value to the agency and the citizens it services. The concept of risk management may be useful. Risk management requires an analysis of risks relative to potential benefits, consideration of alternative measures to address risks, and implementation of the measures that best address the risk based on this analysis. In applying risk management to e-records, the following questions should be asked:

1. What would the impact on agency operations be if the records were lost or otherwise unavailable?
2. Would the agency or others suffer a financial loss if the records were unavailable?
3. What is the likelihood that the records would be subject to or needed for a legal action?
4. Would the inability to produce the records in a form admissible in court have a critical impact on the outcome of a case?
5. Are the records required for an extended period of time?
6. Do the records have significant cultural or historical value?

Interestingly, the guidelines published by the NECCC focus more on the importance of having reliable and accurate processes and procedures used to create, capture, and maintain e-records than on the technology used. Having well established procedures is critical to demonstrating their authenticity, integrity, and security. These factors are much more important than the format or medium of e-records or the specific technology used to create and maintain them. Government agencies should identify, specify, and document these processes and procedures if they expect their e-records to be accepted in legal and other proceedings.

State of Arizona Records Retention Policy

In Arizona, electronic records retention rules are established in A.R.S. § 44-7012 and A.R.S. § 41-1351.

Summary of A.R.S. § 44-7012

A.R.S. 44-7012 establishes that:

A. If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record that:
    1. Accurately reflects the information prescribed in the record after the record was first generated in its final form as an electronic record or otherwise.
    2. Remains accessible for later reference.

B. Subsection A does not apply to any information whose sole purpose is to enable the record to be sent, communicated or received.

C. A person may satisfy subsection A by using the services of another person to satisfy subsection A.
D. If a law requires a record to be presented or retained in its original form, or provides consequences if the record is not presented or retained in its original form, that law is satisfied by an electronic record retained according to subsection A.
E. A record retained as an electronic record pursuant to subsection A satisfies a law that requires a person to retain a record for evidentiary, audit or like purposes, unless a law that is enacted after the effective date of this chapter prohibits the use of an electronic record for the specified purpose.
F. This section does not prohibit a governmental agency from adopting additional requirements for the retention of a record that is subject to that agency's jurisdiction.

Summary of Signature Dynamics Electronic Signing Policy

Retention of digital signature documents is also addressed in the Signature Dynamics Electronic Signing Policy for electronic signature usages created by the Policy Authority of the Office of the Secretary of State (April, 2002). The Electronic Signing Policy is intended for use by State of Arizona agencies, boards, commissions, and their electronic signing partners. It was created by the State of Arizona's Electronic Signature Infrastructure (AESI) and is managed by Arizona's Policy Authority.

In this policy document, under section 5.8.2 "Retention period for Archive," the signing process information must be retained for the "legal" life of the most enduring document signed within the ESI. If that "legal" life is unknown, then it must be kept for at least 30 years. Any signed documents may also have public records retention requirements that must also be met.

Summary of A.R.S. § 41-1351

A.R.S. 41-1351 assigns responsibility for document retention rules to the Arizona State Library, Archives, and Public Records:

> "Every public officer who has public records in the public officer's custody shall consult periodically with the state library and the state library shall determine whether the records in question are of legal, administrative, historical, or other value. Those records determined to be of legal, administrative, historical, or other value shall be preserved. Those records determined to be of no legal, administrative, historical, or other value shall be disposed of by such method as the state library may specify. A report of records destruction that includes a list of all records disposed of shall be filed at least annually with the state library on a form prescribed by the state library."

General Retention Schedule for State Agencies

Specific record retention rule schedules for Arizona state agencies are created and periodically revised by the Arizona State Library, Archives, and Public Records. The most recent revision is dated July 3, 2007 and contains specific guidelines state agencies must follow for retaining documents related to all agency business functions.

Survey of Other States' Departments of Transportation

The fourth task of the Arizona Department of Transportation Digital Signature Feasibility Study required the researchers to survey other states' transportation departments to determine how they are using digital signature technology. The survey started on April 17, 2008, and ended May 2, 2008.

Survey Objectives

1. Understand other states' transportation departments' use of digital signatures and plans to implement the technology in the future.
2. Determine which methods have been used to implement digital signature technology. Identify which software vendors were used and overall satisfaction with those vendors.
3. Understand how well transportation departments have achieved the benefits associated with their digital signature technology implementations (expectations, benefits, implementation challenges).

Jan Edwards, of the American Association of State Highway and Transportation Officials (AASHTO), provided a list of senior level and CIO contacts for every state department of transportation. A survey was developed by the researchers and approved by the study TAC on April 15, 2008 (See Appendix). The questions were converted into an electronic, web-based survey tool. A cover letter was created by AzDOT CIO Joe Throckmorton introducing the survey and asking for help completing it.

The survey was distributed to the transportation departments of 47 states and the District of Columbia. The only states not receiving a survey were Arizona, Ohio, and New York (no DOT contacts were available for Ohio and New York). The survey completion rate was high. In total, the researchers received responses from 36 states (75 percent response rate). Of the 36 responses, 33 included full contact information and three were submitted anonymously. A contact list is provided in Appendix 1.

Survey Results and Findings

Objective 1: Understand use of digital signatures by other states' transportation departments and their plans to implement the technology.

Summary of Findings

The use of digital signature technology is gaining traction with other states' DOTs. More than half the respondents have already implemented the technology (55.6 percent). Of those that have not, over two-thirds (70.5 percent) expect to do so within the next two to three years. Less than a third said they do not see the technology being adopted in the foreseeable future.

For the states not using the technology (44.4 percent of the respondents), the two most commonly cited reasons for not implementing the technology were that the technology

was not considered a priority (50 percent) and that the technology faced legal and regulatory barriers (22 percent).

Digital signature technology is most commonly used to support internal processes (47 percent). This is followed by engineering design and bidding process (26 percent), customer-based processes (19 percent), and other procurement (13 percent).

Key Results:

Table 10: State DOT Survey Results – Objective 1

Question	**Response Percent**
Has your organization implemented any form of digital signature technology?	
YES	55.6%
NO	44.4%
Briefly explain why you have not implemented digital signature technology.	
Not a business priority	50%
Regulatory/Legal issues	22%
Other Reasons	28%
When do you believe your organization will implement some form of digital signature technology?	
Within the next year	41.1%
Within the next 2-3 years	70.5%
Not for the foreseeable future	29.4%
Please select how you are using digital signature technology (select all that apply)	
Customer-based (license renewals, vehicle registration, etc.)	15.8%
Procurement	13%
Engineering & Engineering Bids	26.3%
Internal Processes (timesheets, system access requests)	47.4%
What issues did you have getting your engineers to move to digital signatures?	
Legal/Raised Seal issues	50%
No resistance	33%
Technical issues	17%

Objective 2: Determine which methods have been used to implement digital signature technology. Identify which software vendors were used and overall satisfaction with those vendors.

Summary of Findings

Those states that have already implemented digital signature technology have overwhelmingly selected using third-party software over building customized solutions internally (88.9 percent use third-party software; only 11 percent have built an internal solution). Of the states that have used third-party software, 62.5 percent have purchased software and integrated it into their existing infrastructure (internally hosted) and 37.5 percent have purchased software and have it completely hosted externally.

There was little consistency in the vendors used to implement digital signature technology. There were 10 different vendors named out of a total of 16 responses. Bid Express and VeriSign were named by 20 percent and Silanis was named by 13 percent of the respondents. The respondents are very happy with their vendor selection. Nearly 94 percent of those bought from a vendor said they would recommend the vendor they used. Only one of the 16 respondents would not recommend her current vendor.

Key Results:

Table 11: State DOT Survey Results – Objective 2

Question	**Response Percent**
Please select the method used to implement your digital signature technology.	
Internal customized solution	11.1%
Purchased third-party software/internally hosted	44.4%
Purchased third-party software/externally hosted	33.3%
What third-party provider are you using?	
Bid Express	20%
VeriSign	20%
Silanis	13%
Other	47%
Other vendors named: Lotus Notes, SoftTech, IBM, ViiSAGE, Entrust, UserTrust, InfoTech	
Would you recommend this vendor?	
YES	93.8%
NO	6.3%

The following lists the vendors used by each state and whether the respondent recommended them.

Vendor:	Recommend?	State:
Bid Express	Yes	IN
Bid Express	Yes	MN
Bid Express	Yes	AL
Entrust Digital Certificates/ hosted by the Illinois Central Management Services.	Yes	IL
IBM/FileNet	Yes	NJ
InfoTech	Yes	MI
Lotus Notes	Yes	MO
Silanis	Yes	ND
Silanis	Yes	LA
Silanis (workflow)	Yes	MN
Softech	Yes	NM
UserTrust/Comodo	No	UT
Verisign	Yes	TX
Verisign	Yes	TN
Verisign	Yes	KS
ViiSAGE	Yes	WI

Objective 3: Understand how well departments of transportation have achieved the benefits associated with their digital signature technology implementations (expectations, benefits, implementation challenges).

Summary of Findings

The majority of states that have implemented some form of digital signature technology report their programs have met or exceeded their expectations (72 percent). Because many states have recently implemented their programs, 28 percent reported it was too early to tell. The states, however, are optimistic about their programs' chances of meeting or exceeding expectations. Not a single respondent believed his program wouldn't eventually meet expectations.

The most commonly cited benefit to implementing digital signature technology was improved workflows and shorter times to obtain approvals on internal processes and procurement bids (named by 50 percent). Improved security/authentication was cited as a benefit by 23 percent and 23 percent said their primary benefit has been a reduction in printing and copying costs.

Most states reported facing challenges during and after implementing their digital signature technology programs. Gaining organizational buy-in was cited as the most common challenge (33 percent). Overcoming technical challenges was cited by 29 percent of respondents. It should be noted that 20 percent of the respondents said they

faced no significant challenges. This is somewhat surprising given the complexity of the technical integration and significant changes in business workflows associated with digital signature technology.

Key Results

Table 12: State DOT Survey Results – Objective 3

Question	Response Percent
How would you describe the benefits / savings your project achieved?	
Benefits exceeded expectations	11.1%
Benefits have met expectations	61.1%
Benefits will meet expectations, but haven't yet	11.1%
Benefits will not meet expectations	0%
Too early to tell/no analysis completed	16.7%
What benefits have you realized?	
Improved workflow/shorter approval times	50%
Improved security/authentication	22.7%
Reduced printing	22.7%
Meets legal requirement	4.5%
What challenges did you encounter?	
Gaining organizational buy-in	33%
Overcoming technical challenges	28.6%
No significant challenges	19%
Legal Issues	9.5%
Post-implementation support	9.5%

Survey Conclusion

The Arizona Department of Transportation (AzDOT) has not yet implemented a true digital signature technology program (public/private key digital certificates), but is currently in the process of evaluating the feasibility of doing so. AzDOT is currently using an approval workflow engine called Adobe LiveCycle to support "eForms." The use of this product puts it on par with the majority of states who have implemented some form of electronic approval workflow engine, but who have not implemented pure digital signature technology. A number of states in the survey said they have adopted similar workflow processes, but reported they are not leveraging actual digital signature technology. It should be noted that respondents may have blurred the line between digital signature technology and electronic approval and document management solutions.

Clearly, other DOTs have chosen to buy third-party vendor software over building solutions themselves. This should provide AzDOT with a great opportunity to evaluate

vendor software options and obtain recommendations from other states about their vendor's performance and costs of externally hosting digital certificate processing. As noted in the previous legal review section, there have been a limited number of legal cases about the veracity of digital signatures. The more states that implement the technology the stronger the workflow and legal standing of digital signature should become.

In addition, AzDOT should be able to learn from other states' experience in developing future cost / benefit analysis, implementation strategies, and leveraging lessons experienced by the other implementations. Based on the high response rate for the survey and the fact that 33 states provided contact information for follow-up discussions, AzDOT should be able to leverage its experiences to make its future program more efficient.

The majority of respondents said their programs have performed at or are exceeding the benefits they expected. The remaining states are optimistic about their programs' future performance. These implementations are clearly challenging so it should provide AzDOT with some added confidence that an investment in this technology is worthwhile and has the potential to provide important benefits.

Finally, AzDOT should consider the significant challenges faced by the other states. The most commonly mentioned challenge was gaining organizational buy-in. This challenge is larger than simply "are you using digital signature technology (e.g. digital certificates)?" The challenge speaks more about the difficulty implementing an end-to-end electronic workflow than it is about implementing true digital signature technology. Clearly, an implementation must obtain buy-in from around the entire organization and not be limited to being IT driven.

Advantages/Disadvantages and Cost/Benefit Profile

Section Summary

The fifth task of the Arizona Department of Transportation Digital Signature Feasibility Study required the researchers to document the advantages and disadvantages and cost/benefit profiles for digital signature usage by the department. The TAC also requested a profile of building an in-house digital signature solution versus leveraging a third-party platform. The conclusions reached in this chapter are based on several sources of information including the major findings of the previous sections of this feasibility study (AzDOT interviews, legal review, and findings from the survey of 32 other state departments of transportation), several well documented case studies, and the researchers' personal experience in large-scale technical development.

Research Limitations

There were several limitations that must be noted:

- Interviews with AzDOT staff yielded only a limited set of potential candidate transactions. Those transactions included: timesheets, system access requests, training requests, travel request, and the processes involved in the Engineering bidding and plan drawing process for which a proof-of-concept project is currently in process.

  The researchers learned that most of the internal transactions are already part of AzDOT's eForm initiative. The eForm initiative leverages electronic approval workflow through the Adobe LiveCycle product. The transactions not already on eForms are scheduled to be converted soon.

The conclusions reached in this section are based upon a review of the following materials; each will be described in detail:

1. A review of the legal requirements of digital signature technology,
2. Survey results from 32 other state departments of transportation,
3. Case studies and white papers on the "in-house development" vs. "outsourcing" of digital signature hosting (digital certificate/PKI hosting).

Legal Findings

According to A.R.S § 41-132, Arizona law provides that an electronic signature "may be used to sign a writing on a document that is filed with or by a state agency, board or commission and the electronic signature has the same force and effect as a written

signature." It defines an electronic signature as "an electronic or digital method of identification that is executed or adopted by a person with the intent to be bound by or to authenticate a record." In order to be an electronic signature, it must meet the following three conditions:

(1) Be unique to the person using it,
(2) Be capable of reliable verification,
(3) Be linked to a record in a manner so that if the record is changed the electronic signature is invalidated.

The above referenced portions of A.R.S. § 41-132 were written to be technology neutral and do not prescribe the particular technological approach.

According to the Arizona Electronic Transactions Act, A.R.S. § 44-7001 et seq. (the AETA), Arizona law recognizes that a record or signature in electronic form cannot be denied legal effect and enforceability solely because the record or signature is in electronic form. Arizona law further recognizes that a contract formed by an electronic record cannot be denied legal effect and enforceability solely because an electronic record was used in its formation. Arizona law also provides that an electronic record satisfies any law that requires a record to be in writing. Finally, Arizona law provides that an electronic signature satisfies any law that requires a signature.

The AETA defines a secure electronic signature as one that is:

(1) Unique to the person using it,
(2) Capable of verification,
(3) Under the sole control of the person using it,
(4) Linked to the electronic record so that if the record is changed the electronic signature is invalidated.

These statutes, and each of the requirements set forth for having a valid electronic signature supports the idea that implementing a robust, well documented electronic approval engine will suffice for most, if not all, of AzDOT's previously identified internal transactions without the use of actual PKI technology.

The same statute, A.R.S. § 41-132, defines a digital signature as a "type of electronic signature that transforms a message through the use of an asymmetric cryptosystem."

The requirements of a document containing a digital signature are:

(a) The document must contain a computer based certificate that (1) identifies the issuing entity and the subscriber (the subscriber lawfully holds the private key that corresponds to the public key listed in the certificate and accepts the certificate), (2) contains the subscriber's public key, and (3) is digitally signed by the issuing entity.

The statute does not prescribe when an entity should apply formal digital signature technology over an electronic signature.

A review of the State of Arizona, Policy Authority, Office of Secretary Electronic Signing Policy (April, 2002), (http://www.azsos.gov/pa/SigDynamicsCP) found guidelines that agencies should consider. In section 2.1, agencies must "determine what level of trust (basic, medium, and high) is appropriate for their needs. Applications requiring higher assurance must incorporate a technology approved for those higher levels of trust. This does not preclude using Signature Dynamic signing technologies in circumstances requiring higher levels of trust. It merely requires additional technology to provide the additional trust needed."

Establishing trust levels is based on the potential risk involved and levels of security for the highest risk type of transaction. There are three trust levels:

- **Basic**: There are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.
- **Medium**: Risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.
- **High**: Threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

The Electronic Signing Policy, section 2.4.8.1, (http://www.azsos.gov/pa/SigDynamicsCP), addresses trust levels for:

1. Signer identification (determining the signer is who he says he is),
2. Signer link to signature (his intent to approve something),
3. Signature link to record integrity (ensuring that once signed, a document cannot be changed without invalidating the signature).

There is only a single reference to the use of PKI technology in the policy. Section 2.4.8.1.3 outlines methods for linking an electronic signature to the integrity of the signed record.

> "There must be some method to ensure that the signature is linked to the record content that the signer intended to sign in such a manner that any change to the record since the record was signed is detectable and invalidates the signature."

PKI usage is prescribed only when the high level of trust is warranted. It is our opinion that the high level of trust is not reached for the majority of AzDOT internal forms; however, this reference may be of particular importance to the current effort to develop electronic approval processes for AzDOT Engineering.

Survey Results from 32 Other State Department of Transportation Organizations

Most departments of transportation have overwhelmingly chosen to leverage a third-party vendor for their PKI implementations over building an internally hosted solution (88.9 percent use third-party software; only 11 percent have built an internal solution).

The majority of states using some form of digital signature technology have implemented third-party-approval workflow engines that are not necessarily leveraging true digital signature technology (e.g. not using PKI / Digital certificates). A strategy used by a number of states has been to implement a third-party document management and electronic approval workflow engine to make internal processes like timesheets, system access requests, and some forms of procurement functions more efficient. Integrating these approval engines with a recognized third-party digital certificate issuing authority has been done only when state statutes specifically required the additional security and for transactions classified with higher risk.

Case Study Review: In-House Development Versus Outsourcing Digital Certificate Technology

The following section considers the advantages and disadvantages of developing an internal digital signature/PKI infrastructure versus leveraging a third-party provider. It is the researchers' conclusion that leveraging the expertise and infrastructure of a third-party solution would be the best choice for the Arizona Department of Transportation.

Cost Considerations

The estimates contained in this section apply only to the deployment of a digital signature solution using digital certificates in a full PKI implementation. These estimates do not include an electronic approval workflow engine or document management system. AzDOT has already purchased Adobe's LiveCycle workflow engine.

In-House Development of a Full PKI/Digital Signature Solution

Table 13: High-Level Costs of In-House Development of a PKI Solution

Major Cost Factors	**In-house Development**	**Estimating Assumptions Assumes deployment of 2,000 users**
Development Resources: The cost of IT Staff needed to implement a PKI infrastructure and integrate it into many interfacing systems.	$156,600 (one time)	Assumes 4 FTEs [(1)(2)] (Security Analyst @$40/hr, 3 Client/Server Developers @$35/hr) for 6 months. Calculation: ($40x1080hrs)+(3,240hrs x $35) = $156,600 AzDOT resource costs based on PlanView Primary Role Rates Document (ITG)
Software Costs: PKI software must be purchased to run on internal servers and client PCs.	$87,000 (one time) $17,400 (annual maintenance)	Server based licenses[(1)]: $27,000 Client license[(1)]: $60,000 ($30/client x 2000) Total = $87,000 Maintenance[(1)] = 20%/Yr
New Hardware[(1)]: PKI software typically must run on a dedicated server. Given the size of the AzDOT environment, a very high end server is required. In addition to a primary production server, a secondary server for backup is required. Backup server may also be used for testing. Finally, given the critical nature of digital certificate management, a disaster recovery ("Hot Site") is highly recommended. There will be requirements for incremental telecommunications equipment (routers, firewalls, load	$37,000[(1)] (one time) $7,400 (annual maintenance)	Production Server (4,500) Backup Server (4,500) Disaster Recovery Site (5,000) Telecom equipment: (10,000) Root-Key Mgmt Hardware (13,000) Maintenance[(1)] – 20% Yr

balancers, web servers, database servers; security equipment (access controls, monitoring), and a highly secure root-key management process (hardened token cabinets)		
PKI Consulting Expertise [(2)] Because PKI technology will be new to ADOT IT Staff, it is very likely a PKI expert(s) will be required during the duration of the project. Consultant would be for workflow design as well as technical development/integration work.	$175,000 (one time)	1400 hrs x $125/hr = $175,000 [(2)]
Ongoing Maintenance: Annual FTE cost of maintaining infrastructure and applications.	$109,200 (annual)	1.5 FTE (Technical Support)[(1)] 2080 x 1.5 x $35/hr = $109,200 Assumes a client/server development resource.
Administration Costs: Cost of establishing new users, deleting, maintaining certificates	$78,000 (annual)	1.5 FTE [(1)] 2080 x 1.5 x $25/hr Assumes a Business Analyst level resource
TOTALS **ONE TIME** **ANNUAL**	**$455,600** **$212,000**	
TOTAL 3-YEAR COST	**$1,091,600**	**455,600 x ($212,000 x 3) = $1,091,600**

[(1)] *VeriSign, Total Cost of Ownership for Public Key Infrastructure, White Paper; http://www.verisign.com/authentication/enterprise-authentication/managed-pki/index.html*

[(2)] *Silanis, Build vs. Buy – What to Consider, Webinar; http://www.silanis.com/resource-center/webcasts.html*

[(3)] *Kansas Department of Transportation, 12/18/2006 Price Quotation Sheet*

Integration of a Third-Party Digital Signature/PKI Solution

Table 14: High-Level Costs of Third-Party PKI Solution

Major Cost Factors	**Third Party**	**Estimating Assumptions Assumes deployment of 2,000 users**
Annual Managed Service Fee: Typically an annual fee based for managing a PKI infrastructure at third party (e.g. Maintaining the certificate)	$45,500 (annual) [3]	
User Licenses Vendors typically assign a charge for each certificate issued.	$32,000 (annual) [3]	$16/per license, per year x 2,000 potential users [3]
Initial Setup Fee: Most third parties will charge a one-time setup fee.	$18,000 (one-time) [3]	
Development Resources [1]: The cost of IT Staff needed to implement a PKI infrastructure and integrate it into many interfacing systems.	$19,030 (one-time)	Need internal staff for integration work. Estimated at 1-2 resources for 60 days [1] 1.5 FTEs (1 Developer + .5 Security Analyst) for 60 days (346hrs x $35/hr)+ (173Hrs x $40/hr) = $19,030 AzDOT FTE pricing based on recent PlanView Primary Role Rates for ITG Document
PKI Consulting Expertise [2]: Because PKI technology will be new to ADOT IT Staff, it is very likely a PKI expert(s) will be required for the duration of the project. The consultant would be for workflow design as well as technical development/integration work.	$64,875 (one-time)	1.5 Consultants[2] x 346 hrs x $125/hr = $64,875
Ongoing Maintenance: Annual cost of maintaining infrastructure and applications.	N/A	Typically included in Annual Service Fee

Administration Costs: Cost of establishing new users, deleting, maintaining certificates	$78,000 (annual)	1.5 FTE [(1)] 2080 x 1.5 x $25/hr Assumes a Business Analyst level resource
TOTALS **ONE TIME** **ANNUAL**	 **$101,905** **$155,500**	
TOTAL 3-YEAR COST	**$558,405**	**101,905 x ($155,500 x 3) = $558,405**

[(1)]VeriSign, Total Cost of Ownership for Public Key Infrastructure, White Paper; http://www.verisign.com/authentication/enterprise-authentication/managed-pki/index.html
[(2)] Silanis, Build vs. Buy – What to Consider, Webinar; http://www.silanis.com/resource-center/webcasts.html
[(3)] Kansas Department of Transportation, 12/18/2006 Price Quotation Sheet

There are inherent advantages and disadvantages to in-sourcing development work versus leveraging a third-party digital signature/PKI vendor.

Advantages to leveraging a third-party solution:

Table 15: Advantages to Leveraging a Third-Party Solution

Faster Time to Market	According to the existing case studies, the average implementation for an in-house development project is six months while a typical third-party implementation is 30-60 days.[(1)]
Proven, Mature Solutions	Leverages the experience the vendor has accumulated during many similar implementations across a wide variety of public and private organizations and industries. [(1)]
Legal Opinions	Building a customized solution may expose AzDOT to legal and compliance challenges. Vendors solutions have been audited, reviewed, and tested legally. Vendors may even take some or all of the liability when challenged. [(1)]
Audits	Vendor security procedures and infrastructure are constantly audited. Developing an internal solution may increase AzDOT's exposure to new audits of IT infrastructure, processes, and security practices. [(1)]
Increased emphasis on research and development and maintaining industry/legislative awareness	Companies that specialize in digital signature services are motivated to stay current on fraud and "plug holes." They also remain current on new legislation and adjust their products to remain competitive and relevant in the market place. They may also invest in research and development which would be difficult for AzDOT to make similar investments to keep their in-house development current.

(1)Silanis, Build vs. Buy, Case Study

Disadvantages to leveraging a third-party solution:

Table 16: Disadvantages to Leveraging a Third-Party Solution

Being tied to a particular vendor	AzDOT should consider the difficulty of changing vendors; essentially, a vendor's solution will become embedded into the AzDOT infrastructure and business process. Replacing that vendor will require a significant cost in the re-bidding process, integration, and change management/training should it eventually be replaced.
Lack of flexibility	Vendors are generally reluctant to enhance their applications or change their processes.
Service Level Agreement Management	A relationship management function will need to be created to closely monitor established SLA performance.
System Upgrades/Releases	Vendors periodically enhance their software. When this occurs, customers typically are required to upgrade even if there are no direct benefits gained. This creates additional work in many areas including for development staff who may need to adjust file formats and integrations, acceptance testing, and training.

Advantages of In-house development:

Table 17: Advantages of In-House Development

Flexibility	AzDOT may determine an enhancement may improve a workflow; much easier to assign internal resources than to work with a vendor's change cycle
No Long-Term Dependence on a Third Party	AzDOT has control of its digital signature environment and PKI infrastructure. This includes the possibility that a vendor may de-emphasize PKI, discontinue support of its PKI Software, exit the business, or be acquired by another firm, etc.

Disadvantages of In-house development:

Table 18: Disadvantages of In-House Development

Outside of core expertise	Developing an internal solution may be well outside the development work typically completed by AzDOT IT staff. Having resources focus on non-core capabilities is typically an inefficient development model.(1)
Unknown effort	As a new technology to AzDOT, there is little staff experience to properly assess the complexity of the project, develop accurate plans and estimates, and appropriately manage customer expectations. (1)
Learning Curve	A lengthy learning curve will be experienced during development. The new technology will be highly integrated across the AzDOT infrastructure. Over time, this increases the cost of training new staff and makes turnover of key resources that much more impactful. Having a core development team of 3-4 FTEs means that knowledge will be resident in a limited number of resources. (1)
Opportunity Cost	Because of the lengthy development cycle of six months, the resources devoted to digital signature/PKI rollout could be working on other initiatives, creating a cost when measured against the time of outsourcing. (1)
Changing management priorities	As with any long duration project, priorities change over time that could have a significant impact on successfully implementing an in-house development project.

(1)Silanis, Build Vs. Buy, Case Study

Conclusion

Our conclusion, based on the available sources, is that a well documented, third-party electronic approval workflow application (e.g., Adobe's LiveCycle) or a similar electronic approval workflow engine, provides the necessary structure to make virtually all internal processes and transactions compliant with Federal and Arizona electronic and digital signature guidelines. It is important to note that a robust electronic approval process does not necessarily require the use of formal digital signature technology (e.g., Public/Private key digital certificates). As a reminder, formal digital signature technology is defined as using public-key cryptography, certificate authorities, and other enabling services.

Our conclusion applies to the internal processes/transactions identified throughout this feasibility study including; timesheets, system access requests, travel request and other employee forms. These are commonly referred to as eForms within the department. AzDOT has already rolled out many internal eForms using the Adobe LiveCycle electronic approval workflow application. Others, like timesheets and system access requests are scheduled to be converted into eForms this year. Even more sophisticated transactions, like those used by Engineering (bidding, plan drawing processes) may not require the full use of PKI technology in order to meet Federal and Arizona guidelines. The full use of digital signature technology must be based on an assessment of risk.

AzDOT has not previously been presented with a particularly challenging digital signature project. Most forms are fairly basic, (time sheets, access requests, etc). Engineering has provided the first of many more complex challenges yet to come. If they haven't, AzDOT Leadership needs to complete a formal review and risk assessment of signatures on the various engineering documents. A solution being studied by a current Engineering project team would not use full PKI capabilities. In our opinion, the solution would meet the Secretary of State guidelines of a medium risk transaction.

If AzDOT leadership finds transactions like those used by Engineering or other business applications where the risks or desired levels of trust warrant additional security measures, a full PKI implementation would be a more desirable solution. Leveraging an external third party application is clearly our recommended implementation method. The Adobe LiveCycle product that AzDOT is using has additional modules that can be licensed to provide full PKI capabilities.

Appendix 1: State DOT Personnel that Responded to the Survey

Name:	State:	Email	Phone Number:
Gary Blanton	GA	gblanton@dot.ga.gov	404-656-6034
Mark R. Evans	TX	mevans2@dot.state.tx.us	512-465-7453
Jon Clark	KY	jon.clark@ky.gov	502-564-8900
Robert Ashmore	NM	robert.ashmore@state.nm.us	505-897-7886
Nelson Hill,	FL	nelson.hill@dot.state.fl.us	850-414-4499
Rhonda Ringer	DE	rhonda.ringer@state.de.us	302-760-2607
Tom Westfall	WA	WestfaT@wsdot.wa.gov	360-705-7638
Tom Hurd	VT	tom.hurd@state.vt.us	802-828-3426
Jay Lytle	IN	jlytle@indot.in.gov	317-234-5268
Leon Jackson	DC	leon.jackson@dc.gov	202-741-5384
Doug Couto	MI	coutod@michigan.gov	517-241-2899
Mark D. Kinkade	IL	Mark.Kinkade@Illinois.gov	217-785-2400
Andy Crenshaw	AL	crenshawa@dot.state.al.us	334-242-6264
Dane Prescott	NH	Dane.Prescott@oit.nh.gov	603-271-3281
Mike Bousliman	MT	mbousliman@mt.gov	406-444-6159
Mark Herring	TN	mark.herring@state.tn.us	615-254-6409
Allan Haverkamp	KS	allanh@ksdot.org	785-296-4656
Thomas Kennedy	NJ	thomas.kennedy@dot.state.nj.us	609-530-6252
Renee Ye	UT	rye@utah.gov	801-964-4598
Augustus Wagner	MN	gus.wagner@dot.state.mn.us	651-366-4237
David Allaby	WI	david.allaby@wisconsin.gov	608-26709786
Murali Rao	VA	Murali.Rao@vdot.virginia.gov	804-786-9702
Suzanne Gehring	OR	Suzanne.D.Gehring@odot.state.or.us	503-986-6385
Steven Hulsey	NC	shulsey@dot.state.nc.us	919-707-2201
James E. Yarsky	MD	jyarsky@sha.state.md.us	410-545-8680
Bill Wehling	NE	bill.wehling@nebraska.gov	402-479-3986
Dominic Cali	LA	domcali@dotd.la.gov	225-242.4699
Russ Buchholz	ND	rjbuchholz@nd.gov	701-328-2561
Nancy Armentrout	ME	nancy.armentrout@maine.gov	207-624-3209
CISO	CA	CISO@dot.ca.gov	916-653-0972
Ken Slay	MS	kslay@mdot.state.ms.us	601-359-9829
Bryan Stewart	AR	bryan.stewart@arkansashighways.com	501-569-2436
Todd Walters	MO	todd.walters@modot.mo.gov	573-526-3164

Appendix 2: Survey Questions

The following survey was used to obtain input from the other states' DOT.

	QUESTION	**ANSWER**
1	Has your organization implemented any form of Digital Signature Technology?	Yes / No
	If answer is yes, the survey will automatically skip to question 4	
	If answer is no, the survey will move to the following questions	
2	Please briefly explain why you have not implemented Digital Signature Technology.	FREE FORM TEXT BOX
3	When do you believe your organization will implement some form of Digital Signature Technology?	a. Less than a year b. Within the next year c. Within the next 2-3 years d. Not in the foreseeable future
	For the "No digital signature path" - The survey will ask for the name/phone number of someone we can contact later. The survey will thank them for their time.	
	Digital Signature "YES" path	
4	Please select how you are using Digital Signature Technology (select all that apply)	Select all that apply: a. Customer-based (license renewals, vehicle registration, etc.) b. Procurement c. Engineering d. Internal processes (timesheets, system access requests, etc.) e. Other: OPEN A Free Form Text Box
5	Please select the method used to implement your Digital Signature Technology	a. Internal customized solution b. Purchased 3rd party software / internally hosted (runs on your organization's infrastructure) c. Externally hosted by a third party provider (does not run on your organization's infrastructure)

	QUESTION	**ANSWER**
5a	What third party provider are you using? -- **This opens only if they select b or c on question 5**	FREE FORM TEXT BOX Vendor contact information
5b	Would you recommend this vendor?	YES / NO
6	How would you describe the benefits / savings your project has achieved	a. Benefits have exceeded our expectations b. Benefits have met our expectations c. Benefits will meet expectations, but haven't yet d. Benefits will not met expectations e. Too early to tell / No post-implementation analysis has been completed.
7	What benefits have you realized?	FREE FORM TEXT BOX
8	What major challenges did you encounter?	FREE FORM TEXT BOX
9	We would like to include the information that you provided in our study. We might also contact you for clarifications. Please provide us with some information about yourself.	TEXT BOX FOR NAME, EMAIL, PHONE