Increasing the Speed of Signature through Technology

May 16, 2011

Project Summary

Governor John Kasich has repeatedly stated that Ohio must operate at the speed of business in order to remain competitive: "we need to move quickly in every area, because business moves at the speed of light (state of Ohio, 2011)." The implementation of paperless document processes, particularly digital signatures, is one way to achieve this goal. Digital signatures are "the most effective, secure, and easy-to-implement method of providing accountability while enabling electronic transactions (Entrust, 2003)." Paperless document processes save time and money by:

- Reducing paper handling, including copying, scanning, filing, faxing, and shredding
- Reducing errors associated with common paper related tasks
- Eliminating costs for paper, paper storage, and postage
- Expanding document access
- Streamlining document processing
- Improving service and convenience for state customers and vendors

Project Goal

This paper will provide an explanation of terms relevant to digital signatures, describe the current use of such technology within both the state of Ohio and the federal government, provide case studies of three states that have explored or implemented digital signature technology, and make recommendations should Ohio choose to explore the implementation of digital signatures as one way to achieve the goal of pushing government to operate at the speed of business.

Project Outcome

In order for Ohio to be competitive in the global market, the state must establish an infrastructure that supports digital signatures and paperless processes. This paper has examined the technology, legal environment, and use of digital signatures in Ohio and other states. It recommends that Ohio update its current policies in light of today's security threats and business opportunities. The existing administrative rule governing the use of electronic signatures has not been updated since 2007 and should be reviewed, particularly to determine whether it needs to be amended to eliminate unnecessary paperwork (ORC section 119.032(C)(3)). This paper proposes that a governance group be created to oversee the policies, decision-making, and implementation efforts necessary to establish a PKI for use within the state. It also recommends that the state incorporate the requirements necessary to tie into similar efforts at the federal level (FPKI). Finally, it recommends that the state should actively review the systems accessed through the Ohio Business Gateway to determine if digital signature technology is appropriate.

Project Benefits

With state of Ohio agencies facing a future of shrinking budgets and resources, many are exploring ways to streamline business processes. One way is through the implementation of paperless document processes, including electronic document storage and electronic transaction processing for employees, vendors, and the state at large. For Ohio agencies to fully realize a paperless environment, they must integrate digital signature technology as part of their electronic document processes.

The cost of a handwritten signature is estimated to range between $5.40 and $30 (McLaughlin, 2007; Lantsman, n.d.). These costs take into account factors such as length of document, scanning, storage, workflow disruption, and loss/reproduction.

Digital signature technology results in time and cost savings in the following ways:

- Reduced paper handling, including copying, scanning, filing, faxing, and shredding
- Reduced errors associated with common paper related tasks
- Reduced cost for paper, paper storage, and postage
- Streamlined document access
- Faster document processing
- Improved service and greater convenience for state customers and vendors

Project Team

For more information about this project, contact team members

- Darryl Morrison — Darryl.Morrison@dps.ohio.gov
- Deb Daugherty — Debra.Daugherty@das.ohio.gov
- Korrina Thomas — Korrina.Thomas@obm.state.oh.us
- Julie Hartzell — Julie.Hartzell@lsc.ohio.gov
- Sydney Waugh — Sydney.Waugh@das.state.oh.us
- Yancy Wessell — Yancy.Wessell@dot.state.oh.us
- Mentor/Coach – Nelson Gonzalez

Increasing the Speed of Signature through Technology

Team Quick Sign

Executive Summary

Governor John Kasich has repeatedly stated that Ohio must operate at the speed of business in order to remain competitive: “we need to move quickly in every area, because business moves at the speed of light (state of Ohio, 2011).” The implementation of paperless document processes, particularly digital signatures, is one way to achieve this goal. Digital signatures are “the most effective, secure, and easy-to-implement method of providing accountability while enabling electronic transactions (Entrust, 2003).” Paperless document processes save time and money by:

- Reducing paper handling, including copying, scanning, filing, faxing, and shredding
- Reducing errors associated with common paper related tasks
- Eliminating costs for paper, paper storage, and postage
- Expanding document access
- Streamlining document processing
- Improving service and convenience for state customers and vendors

For Ohio agencies to fully realize the benefits of a paperless environment, they must integrate electronic signature functionality as part of their electronic document processes. To do so effectively, several initial steps should be taken. First, the existing administrative rule governing the use of electronic signatures, which has not been updated since 2007, should be reviewed to determine whether unnecessary paperwork can be eliminated for agencies implementing this capability. Next, a governance group should be established to direct the policy, decision-making, and implementation efforts necessary to build and/or procure digital signature solutions. The group should review and ensure the state of Ohio meets the federal digital signature standards, in order to benefit from interoperability with federal systems. Finally, it is recommended that the state of Ohio should evaluate the systems accessed through the Ohio Business Gateway website, to determine if the introduction of digital signature technology through this venue is an appropriate and logical step.

In order to fully comprehend the different types of electronic signatures, it is important to have a common understanding of the terms associated with this technology. A **wet signature** is the traditional handwritten signature used to identify the source and intent of the signer. A **digitized signature** is a graphical image of the wet signature generally created by scanning a wet signature and is the digital equivalent of the rubber stamp. An **electronic signature** is defined by the state as “an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record (ORC section 1306.01(H)). A **digital signature** is a type of electronic signature that ensures data integrity, confidentiality, identification and authentication, and non-repudiation through a cryptographic system. One of the most common cryptographic systems in use is **Public Key Infrastructure (PKI)**, consisting of policies, processes, and technology used to administer certificates and keys required to encrypt and decrypt information.

Today, at least 14 state of Ohio agencies have incorporated some sort of electronic signature technology into their business processes. In 2004, Ohio’s Office of Information Technology (OIT) explored a possible enterprise approach for implementing a PKI system, but found the cost to build and maintain such a system without either a mandate or a strong business case to be too high. While Ohio Administrative Code rule 123:3-1-01 recognizes electronic transactions as equivalent to paper-based transactions, it also requires state agencies to document electronic transaction use, and complete transaction risk assessments. The purpose of the

transaction risk assessment is to classify electronic transactions into one of four security levels, and assign minimum requirements for the transaction authentication, integrity, and non-repudiation.

In response to numerous acts, including the Health Insurance and Portability and Accountability Act of 1996 (HIPAA), the Government Paperwork Elimination Act of 1998 (GPEA), the Uniform Electronic Transactions Act (UETA), and the Electronic Signature in Global and National Commerce Act (ESIGN), the federal government established the Federal PKI (FPKI), which allows federal and state agencies greater flexibility in making the "build or buy" PKI decision, as well as interoperability between entities that are FPKI certified.

Other states, including Illinois, North Carolina, and Virginia, have explored or implemented digital signature systems. Illinois spent approximately $700,000 to establish its own PKI environment and is currently the only state to be cross-certified with the FPKI. The Illinois PKI is managed by the Department of Central Management Services, which provides centralized services for state agencies. Among others, Illinois cites seamless service to citizens and businesses, streamlined transactions, improved public access, and enterprise-wide compatibility as some of the key benefits of their implementation method.

North Carolina has been exploring digital signature functionality since the 1990s, and today electronic and digital signatures are in limited use by the state. A 2008 pilot program identified potential savings through reduced document storage and retrieval costs, lower costs for document routing, fewer delays in document processing, and reduced printing and distribution costs associated with paper forms.

After much consideration, Virginia chose to use a third party PKI provider rather than establish its own PKI environment. The implementation costs using this method were virtually none. The vendor agreed to create custom webpages for the state, where vendors, customers, and employees could apply and pay for their digital certificates, which cost an applicant $119 for a two-year certificate. Benefits realized by Virginia from the implementation of digital signature functionality included improved efficiency through streamlined cycle times, improved reputation with the business community, and an improved business climate within state government.

Based on the information gathered for each state, there are three questions to ask when considering the implementation of digital signature technology. First, build or buy? Building a system from ground up is an expensive investment that requires regular maintenance, while third party providers can be highly cost effective. However, given the potential fallout states might experience with a security breach, it might be more reassuring to maintain a PKI environment in-house. Second, should the state bridge to the FPKI? Interoperability with federal systems and adherence to federal standards and mandates is critical to most state governments. As such, states should either pursue cross-certification as part of their initial implementation project, or else they should ensure that their system will be cross-certified at a later date. Finally, are the state's current statutes conducive to implementing digital signature technology? As previously mentioned, OIT has explored the implementation of digital signatures in the past, but has yet to be presented with either a good business case or a mandate to do so.

Table of Contents

Executive Summary 2
Introduction / Purpose 5
Benefits / Business Case 5
Explanation of Terms 6
Federal 10
Current State 10
Relevant Law 10
Case Studies 12
Illinois 12
North Carolina 14
Commonwealth of Virginia 16
Considerations 18
Next Steps / Recommendations 18
References 21
Transaction 44
Electronic Records 44

Introduction / Purpose

Governor Kasich has repeatedly stated that Ohio must operate at the speed of business in order to remain competitive: “we need to move quickly in every area, because business moves at the speed of light (state of Ohio, 2011).” The implementation of paperless document processes, particularly digital signatures, is one way to achieve this goal. Digital signatures are “the most effective, secure, and easy-to-implement method of providing accountability while enabling electronic transactions (Entrust, 2003).” Paperless document processes save time and money by reducing errors and common paper related tasks, and by streamlining access to documents. This technology also reduces processing wait times, thereby increasing customer satisfaction. When properly implemented, digital signatures are legal and binding, affording electronic transactions the same legitimacy as paper transactions. Ohio will not gain a competitive edge until it is faster and more convenient to do business with the state.

This paper will provide an explanation of terms relevant to digital signatures, describe the current use of such technology within both the state of Ohio and the federal government, provide case studies of three states that have explored or implemented digital signature technology, and make recommendations should Ohio choose to explore the implementation of digital signatures as one way to achieve the goal of pushing government to operate at the speed of business.

Benefits / Business Case

With state of Ohio agencies facing a future of shrinking budgets and resources, many are exploring ways to streamline business processes. One way is through the implementation of paperless document processes, including electronic document storage and electronic transaction processing for employees, vendors, and the state at large. For Ohio agencies to fully realize a paperless environment, they must integrate digital signature technology as part of their electronic document processes.

The cost of a handwritten signature is estimated to range between $5.40 and $30 (McLaughlin, 2007; Lantsman, n.d.). These costs take into account factors such as length of document, scanning, storage, workflow disruption, and loss/reproduction.

Digital signature technology results in time and cost savings in the following ways:

- Reduced paper handling, including copying, scanning, filing, faxing, and shredding
- Reduced errors associated with common paper related tasks
- Reduced cost for paper, paper storage, and postage
- Streamlined document access
- Faster document processing
- Improved service and greater convenience for state customers and vendors

Explanation of Terms

The purpose of this section is to provide common definitions for terms associated with digital signature technology. For a more comprehensive glossary of digital signature terms and concepts, refer to either Appendix A or specifically cited sources as appropriate.

A **signature** is defined as "a person's name or a mark representing it, as signed personally or by deputy, as in subscribing a letter or other document (Dictionary.com, n.d.)." This is sometimes referred to as a handwritten or "wet" signature. A wet signature generally serves two primary functions. The first is to uniquely identify the source of the signature. The second commonly used function is to identify intent. A common example of a wet signature is when a person signs a contract, clearly indicating "who" the contract involves and the signer's "intent" to be bound by the agreement. Since the wet signature has been in use for a long period of time, there is a large body of law which regulates its use.

A **digitized signature** is a graphical image of a wet signature, generally created by scanning the wet signature. Since anyone can easily insert a digitized signature into a document, it is difficult to determine exactly who signed the document. A digitized signature is the digital equivalent of the "rubber stamp" or "facsimile signature."

An **electronic signature** can be considered the first attempt to provide a legally binding digital equivalent of a wet signature. Ohio Revised Code (ORC) section 1306.01(H) defines an electronic signature as "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." At the federal level, it is defined as any method of signing an electronic message that identifies and authenticates the person who is the source of the message and indicates that person's approval of the contents (Government Paperwork Elimination Act,1998; NIST SP 800-32).

A **digital signature** can be considered a more secure version of an electronic signature. ORC section 1733.29(H)(2)(d), related to credit union law, defines a "digital signature" as an encrypted electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature. Digital signature is not defined in any other section of the ORC.

The National Institute of Standards and Technology (NIST) defines a "digital signature" as:

> The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made (NIST SP 800-32).

NIST associates the following basic security services with digital signatures:

> **Data integrity** services address the unauthorized or accidental modification of data. This includes data insertion, deletion, and modification. To ensure data integrity, a system must be able to detect unauthorized data modification. The goal is for the receiver of the data to verify that the data has not been altered.

Confidentiality services restrict access to the content of sensitive data to only those individuals who are authorized to view the data. Confidentiality measures prevent the unauthorized disclosure of information to unauthorized individuals or processes.

Identification and authentication services establish the validity of a transmission, message, and its originator. The goal is for the receiver of the data to determine its origin.

Non-repudiation services prevent an individual from denying that previous actions had been performed. The goal is to ensure that the recipient of the data is assured of the sender's identity.

Cryptography is a branch of applied mathematics concerned with transformations of data for security purposes (NIST SP 800-32).

Public Key Infrastructure (PKI) is a set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates (NIST SP 800-32).

In the public-private key pair, the **private key** is used to create a digital signature and decrypt confidential information, and must always be kept secret. The **public key** is used to validate a digital signature and encrypt confidential information, and is typically made publicly available through digital certificates.

A user's private key can be stored on a computer, but a more portable option is to store the key on a smart card. A **smart card** is a wallet-sized card, often tamper-resistant, with embedded integrated circuits that can store, process, and communicate information (NIST IR-7298).

A **Certification Authority** (CA) is an entity that issues digital certificates to subscribers. The CA acts as a trusted third party, certifying the identity of the subscriber to anyone who receives a digitally signed message (Washington Secretary of State, n.d.).

Current State and Relevant Laws

Ohio

Current State

PKI is not a new concept to the state of Ohio. In 2004, Ohio's Office of Information Technology (OIT) explored a possible enterprise approach for implementing PKI technology to "manage and protect the trust between citizens, businesses and government in an electronic world (p. 1)." OIT recognized the inherent value of PKI as a means to propel the state forward in its pursuit of electronic business and service solutions. However, also noted were the significant start-up and maintenance costs associated with PKI technology. OIT concluded that until a business case—either agency or enterprise—can show that the value of PKI is greater than the total cost of implementation and maintenance, or until there is an explicit legal mandate, there is no demonstrated need to pursue this technology.

Today, at least 14 state agencies use some sort of electronic signature functionality, based on information obtained from OIT (for a complete list, see Appendix B). Unfortunately, there is no way to know what systems are in place, if they are compatible, or if the transaction types are similar. Furthermore, it is possible that other Ohio agencies have implemented some sort of electronic signature functionality, but have not been required to file with OIT, pursuant to Ohio Administrative Code (OAC) rule 123:3-1-01, which requires electronic transaction reports to be completed prior to implementing certain types of electronic signature capabilities.

Relevant Law

In 2000, the General Assembly enacted sections 1306.01 to 1306.23 of the Revised Code, known as the Uniform Electronic Transactions Act (Sub. H.B. 488, 123rd General Assembly). This act, among other things, provided for electronic record and electronic signature use by state agencies and required the Department of Administrative Services (DAS) to adopt rules for such use. ORC section 1306.01(H) defines "electronic signature" as an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. The act is not mandatory, as nothing in the act's provisions requires any state agency to use or permit the use of electronic records and electronic signatures.

ORC section 1306.06 specifies that (1) a record or signature may not be denied legal effect or enforceability solely because it is in electronic form, (2) a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation, (3) if a law requires a record to be in writing, an electronic record satisfies the law, and (4) if a law requires a signature, an electronic signature satisfies the law. ORC section 1306.12 states that evidence of a record or signature may not be excluded in a proceeding solely because it is in electronic form. Whether an electronic record or electronic signature has legal consequences is to be determined by the provisions of the act and other applicable law, as provided by ORC section 1306.04. Pursuant to ORC section 1306.20, state agencies must determine if, and the extent to which, they will send and receive electronic signatures to and from other persons and otherwise create, generate, communicate, store, process, use, and rely upon electronic signatures.

ORC section 1306.21 required DAS to prescribe administrative rules governing the use of electronic records and electronic signatures that, under specified circumstances, must be complied with by any state agency that creates, uses, receives, or retains electronic records or creates, uses, or receives electronic signatures. Pursuant to this requirement, DAS adopted OAC rule 123:3-1-01, effective 12/13/2000.

OAC rule 123:3-1-01 states, "Electronic transactions have the equivalent level of legal protection that is given to paper-based transactions. All security procedures and technologies should provide authentication, nonrepudiation and integrity to the extent that is reasonable for each electronic transaction." It also requires state agencies to: document uses of electronic transactions; conduct a transaction risk assessment of each set of similar electronic transactions; use, as a minimum, technology standards and/or security procedures that are appropriate for the level of transaction risk as determined by the security assessment; establish and maintain documented security policies and procedures; and seek a waiver from OIT if the state agency determines that the security technologies or procedures do not conform to the minimum technology standards as established by this rule for the level of security identified in the transaction risk assessment.

OAC rule 123:3-1-01 Transaction Risk Assessment. The purpose of the transaction risk assessment required by OAC rule 123:3-1-01(C)(2)(b) is to classify transactions at an appropriate security level. The risk assessment includes both the probability and impact of a security breach. In determining the impact, agencies should consider the intended use and type of information involved, the degree of risk and legal liability to the state, users, and third parties, the volume and network used for the transactions, the estimated costs, and the appropriate requirements for identity authentication. The rule includes specific language to be used in evaluating the probability and impact of a security breach and is included in Appendix C. A copy of the Electronic Transaction Report used for the risk assessment is included in Appendix D.

The end result is that a transaction will be classified into one of four security levels. To illustrate the process of classifying transactions, a Transaction Risk Decision Matrix was created and can be found in Appendix E.

Federal

Current State

At the federal level, the technological aspects of electronic signature transactions are the responsibility of NIST. NIST researches, develops standards, and promotes the use of PKI in implementing secure electronic signature transactions. Procurement of PKI services is aided by the General Services Administration (GSA), which administers the Access Certificates for Electronic Services (ACES) program. The ACES program is a convenient PKI procurement method for federal and state agencies that do not want to develop their own internal systems (NIST SP 800-25).

A Federal Public Key Infrastructure (FPKI) was developed and uses a distributed technology and certificate authority (CA) model to support interoperability between an organization's PKI, a PKI provided by a commercial service, or a bridge CA serving a community of interest. This design allows federal and state agencies greater flexibility in making the "build or buy" PKI decision. The FPKI is evolving, but there are significant benefits to adopting the FPKI standards. For state governments, interoperability with federal systems and support for new federal standards and mandates is vital.

Relevant Law

There is a long history of working to promote and implement secure electronic transactions at the national level. The Health Insurance and Portability and Accountability Act of 1996 (HIPAA) was designed to improve efficiency through the use of uniform electronic data exchange mechanisms for health information. To achieve this, HIPAA required electronic processing and transmission of administrative and financial healthcare information. The methods used to protect this information later became known as the HIPAA Security Rule (NIST SP 800-66 - Revision 1).

In 1998 the Government Paperwork Elimination Act (GPEA) required federal agencies to provide an option to submit information or perform transactions electronically. The GPEA specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form, and encourages federal government use of a range of electronic signature alternatives (NIST SP 800-25).

In 1999, the National Conference of Commissioners on Uniform State Laws developed a model law to be adopted at the state level known as the Uniform Electronic Transactions Act (UETA). This model law has been enacted by all but three states and "establishes the legal equivalence of electronic records and signatures with paper writings and manually-signed signatures, removing barriers to electronic commerce (National Conference of Commissioners on Uniform Sate Laws, 2010)." Similarly, the Electronic Signatures in Global and National Commerce Act (ESIGN) was signed in 2000 to establish the legal validity of electronic contracts, records, and signatures in interstate and international commerce (Federal Trade Commission, 2001).

In 2004, Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors was put into effect. This directive resulted in the implementation of a new standardized identity badge designed to enhance

security, reduce identity fraud, and protect personal privacy (Department of Homeland Security, 2011).

Case Studies

Illinois

Approach/Background

Illinois established a PKI environment providing authentication, encryption, and digital signature capabilities available to any governmental entity in January 2001. The Illinois PKI is managed by the Department of Central Management Services, which provides centralized services for state agencies. The Illinois PKI incorporates Entrust software for the CA, Siemens for the Directory, and other Entrust products for desktop and portal applications. In 2003, the state of Illinois was the first, and remains the only, state to cross-certify with the Federal PKI (S. Bishop, personal communication, March 29, 2011).

Scope

Current functions utilizing PKI in the state of Illinois are:

- Accessing the Health & Family Services Medi system to check on Medicare claims.
- Accessing the Department of Aging website check on benefits for the elderly.
- Filing electronic water discharge reports to the Environmental Protection Agency.
- Providing encrypted background checks to schools, etc, using the Illinois State Police CHRI system.
- Obtaining teacher education scholarship information and digitally signing applications via the ISAC “CollegeZone” website.
- Viewing filings and board opinions of the Pollution Control Board.
- Securing email for Illinois State University.
- Providing access to legacy applications through the Internet.
- Kane County Circuit Clerk’s office utilizing digital signatures on biometric flash drives for use by judges.
- Digitally signing internal forms by the Illinois Department of Transportation.
- Providing digital signing and encryption capabilities for administrative personnel at Southern Illinois University at Carbondale.
- Digital signing of police reports by the City of Rock Island.
- Providing encrypted email for Central Management Services.
- Sharing sensitive information via encryption by the Office of the Auditor General.
- Sharing sensitive information via encryption/encrypted email for the Office of the Executive Inspector General.
- Provide PIV credentials to first responders (S. Bishop, personal communication, March 29, 2011).

Cost

The initial implementation cost in the state of Illinois was approximately $700,000 for the hardware and professional services. Maintenance costs include $85,000 annually for audits, plus additional contract fees (G. Wells, personal communication, April 14, 2011).

Benefit

- Provides seamless service to citizens and businesses.
- Contributes to the state's goal to continue to develop and deploy initiatives aimed at increasing accessibility, ensuring privacy, strengthening security, authenticating individuals in the deployment of e-government initiatives, and ensuring compatibility across the enterprise.
- Streamlines online transactions and improves public access to agency services.
- Cross-certification with the FPKI paves the way for easier interaction between state and federal agencies.
- The infrastructure allows state agencies to provide secure internet-enabled sites that allow a high-level of authentication to applications, secure encryption capabilities, and digital signing of documents, thus providing better service to the citizens and greater savings to the agencies (S. Bishop, personal communication, March 29, 2011).

Lessons Learned

Recommendations from Illinois based on that state's experience:

- Implement a flat directory structure.
- Implement a tracking tool to determine who has the client loaded on their desktops so the state can contact them when the client software changes.
- Illinois has customers all over the United States with the client and the state will be changing to a SHA-256 cert. At that time, the old client will not work and the only way to find these people will be when they call and say it does not work.
- Implement an online registration and recovery system from the beginning. Illinois has some users that were created manually and some that were automated. The manual users still have to be recovered manually and it causes additional time resource issues (G. Wells, personal communication, April 14, 2011).

Statutes and Rules

- Electronic Commerce Security Act 5 ILL. COMP. STAT. 175
- Administrative Order No. 1 (2002)
- ILL. ADMIN. CODE tit. 14, § 105

North Carolina

Approach/Background

In the 1990s, the North Carolina Office of Information Technology Services and the North Carolina Secretary of State's Office developed a digital signature pilot program to demonstrate that e-signatures were feasible in state government. However, the project did not move beyond the pilot program at that time because of the cost of infrastructure and other issues.

Another pilot program was developed in 2008 to study implementation of an electronic document management system that included digital signature capability. The intent of the study was to demonstrate a technical proof of concept for e-forms with a digital signature.

Electronic and digital signatures are in limited use in the state today (e-notary program, filing of real estate records). While the state understands the increased convenience to citizens for the conduct business with the state if digital signatures are implemented on a broader basis, such a system remains a challenge due to the state's current budget situation (Bakolia, 2009).

Scope

As a first step, the North Carolina Office of Budget and Management is working with other state agencies to compile an inventory of all paper and electronic forms currently in use by executive branch agencies.

Cost

The 2008 pilot identified the following potential cost savings:

- Potentially reduce the cost of licenses and support for electronic document and records management with a statewide, as opposed to agency-based, approach.
- Reduce printing costs by eliminating most paper forms and replacing them with online forms. The research firm Gartner estimates that moving from paper forms to distributed electronic versions that can be printed out and filled in can save up to $14 per form in printing, storage, and distribution costs. A more comprehensive approach to fill, validate, sign, submit and manage a form can save of as much as $150 per form.
- Reduce storage and retrieval costs by eliminating most paper forms. As an example, one relatively small agency currently has three off-site storage units that are used to store boxes of file folders containing inactive material that is required to be maintained until the records retention and legal storage requirements are met.
- Reduce document distribution and routing costs and delays in processing.
- Reduce the loss of files and risks of violations of regulatory, security or privacy acts (Bakolia, 2009, p. 9).

Benefit

Based on the pilot programs, the following were identified as potential productivity and efficiency gains:

- A reduction in manual data entry—state employees currently key material that was originally created electronically. If they accepted the information directly, errors resulting from re-keying information could be eliminated.
- A reduction of e-mails and conversations focused on gathering complete information about a client or business rather than finding a complete electronic file when needed (when access is authorized).
- A reduction in the cost of processing cash receipts and checks by moving to electronic funds transfer. This can also lead to an increase in deposits by the elimination of "float" time.
- A reduction in the cost of mailing materials.
- Quicker response from state agencies to inquiries and applications.
- Depending on how the systems are implemented, citizens may be able to track applications through the work flow to determine when a permit will be issued, or if additional information is needed (Bakolia, p. 9-10).

Statutes and Rules

- North Carolina Electronic Commerce Act N.C. GEN. STAT. § 66-58.1
- North Carolina Uniform Electronic Transaction Act N.C. GEN. STAT. § 66-311
- N.C. ADMIN CODE tit. 18, r. 10.0100-.0900

Commonwealth of Virginia

Approach/Background

In 2008 the Commonwealth of Virginia began exploring ways to implement digital signature technology within the state. Two agencies, the Department of Mines and Minerals and Energy (DMME) and the Virginia Department of Transport (VDOT) were identified for the state's pilot implementation, as each had demonstrated a business need for this functionality.

Initially the project team focused on establishing the PKI environment within the Commonwealth. However, after six months of research and little progress to show, the team determined that the cost to do so far outweighed the benefits. The team switched gears and began looking into third party PKI providers. Shortly thereafter the team agreed on IdenTrust, a provider that offers the ACES Program (A. Rohatgi, personal communication, April 18, 2011). The ACES Program offers digital signature technology specifically for individuals and organizations that conduct business with federal and state government agencies. IdenTrust was the first ACES Certificate Authority identified by the United States GSA (Identrust, n.d.).

Scope

As part of the pilot implementation, the project team identified three broad transaction types—business to government, individual to government, and government to government and/or business. The focus of the project was narrowed to exclude individual to government transactions, as well as most government to government and/or business transactions. The assumption was that different transaction types have different requirements, and a good approach moving forward would be to phase in the various transaction types based on the outcome of the pilot implementation.

Specifically, the scope of the pilot implementation was as follows:

1. Situations that require businesses to submit documents that require a wet signature and possibly a professional seal with wet signatures for legal or statutory purposes. Document types include, but are not limited to, engineering drawings and maps. The formats included will be .pdf, .doc, or .tiff.

2. Situations that require state employees to certify documents with a wet signature and a professional seal for legal or statutory purposes. Document types include, but are not limited to, engineering drawings and maps. The formats included will be .pdf, .doc, or .tiff (Rohatgi, 2008).

Cost

The cost to Virginia to implement digital signatures using IdenTrust was virtually none. IdenTrust agreed to create custom web pages where DMME and VDOT customers, vendors, and employees could apply and pay for their digital certificates. One of the reasons the project team focused on private organizations that do business with Virginia was because they could easily absorb the cost of the digital certificates, and it would be of great benefit for them to do so. VDOT chose to offer digital signature certificates to its employees, at the cost of $119 for each two-year certificate.

In addition to the digital certificate, organizations that do business with Virginia were required to possess or procure software to create an interface for their digital signatures, such as ADOBE LiveCycle.

The minimal costs Virginia incurred as part of this pilot project were for the development of training materials for VDOT employees and entities doing business with the state.

Benefits

The project team identified key benefits associated with the implementation of a digital signature solution:

- Improved efficiency through streamlined cycle times
- Improved reputation within the business community
- Improved business climate within the Commonwealth
- Significant cost savings, both for Virginia and its vendors and contractors

Statutes

- VA CODE ANN. § 59.1-496 Acceptance and distribution of electronic records by public bodies; electronic filing of information permitted
- VA CODE ANN. § 59.1-490 Retention of electronic record
- VA CODE ANN. § 59.1-492 Automated transactions

Considerations

There are three questions state governments and agencies should consider when they think about implementing digital signature technology.

Question 1: Build or buy? The cost to implement an in-house digital signature solution can range from $130,000 to $700,000, not including annual maintenance costs, which can cost from $60,000 to more than $200,000 a year (Entrust 2009). Procuring the services of a third party vendor through the Federal ACES program could be done "at little or no cost for agencies to immediately utilize digital signature technology in their business processes (Identrust, 2009)." Identrust asserts that until now, the lack of a low-cost solution for digital signatures has been the biggest barrier for small to medium-sized companies and public organizations.

Question 2: Bridge to the FPKI Policy Authority (FPKIPA) or not? As stated previously, the FPKI is still a work in progress, but for state governments, interoperability with federal systems and support for new federal standards and mandates is vital. As such, states should either plan to be cross-certified with the FPKIPA as part of their initial digital signature implementation project, or ensure that their system can be cross-certified at a future date.

Requirements for FPKI cross-certification can be found on the FPKIPA website (http://www.idmanagement.gov/fpkipa), and the FPKIPA will work with applicants through the cross-certification process.

Question 3: Are current statutes conducive to the implementation of digital signature technology? As mentioned above, ORC section 1306.21 required DAS to prescribe administrative rules governing the use of electronic records and signatures, the details of which are found in OAC rule 123:3-1-01. This rule requires agencies to document how they use or plan to use electronic transactions, complete a transaction risk assessment, and submit the assessment for certain electronic transaction types. While the rule includes the option for agency use of PKI technology, it must be first be approved by OIT. To date, OIT has not been presented with a good business case to implement PKI at either the agency level or statewide.

Next Steps / Recommendations

There is an increasing trend for the use of electronic signatures in government as well as private sector industries. Although the case studies included in this paper raise some caution as to the cost and effort of implementation, there will be a continued demand for this capability in the state of Ohio.

Should the state of Ohio decide that there is a need for the expanded use of electronic signatures or for the implementation of digital signatures, the recommended first step is to form a state committee to explore the build/purchase decision and the best strategy for implementation of a statewide system. The committee should include representatives from key agencies, including, but not limited to, the state Chief Information Officer and representatives from business-facing agencies such as the Department of Taxation and the Secretary of State's Office. It is also important to include agency representatives that bring technical and legal expertise.

OIT referenced the third party trust model in its findings, and described the need for a certificate authority to issue and ensure the legitimacy of public and private keys (Ohio Department of Administrative Services, Office of Statewide IT Policy, 2004). In fact, OIT recognized the state of Ohio as fulfilling the role of the third party trust broker should PKI technology be pursued. When exploring an enterprise approach for PKI technology, it appears as though OIT did not consider using a non-state of Ohio third party PKI provider. However, there is a need for the state to have a certificate authority to issue and ensure the legitimacy of public and private keys. Therefore, it is recommended that the state explore third party PKI provider options that could best fit the needs of the state.

Other recommendations include:

- The state should implement a system that can bridge to the Federal PKI.
- The state should focus on key projects and/or identify pilot agencies or transaction types. Exploring the current technology practices of the Ohio Business Gateway might be a good starting point.
- The state should poll all agencies to identify possible current and future uses of such technology.

Possible areas of implementation and/or improvement might include:

- First responders / law enforcement
    - Implementation of PKI would facilitate the seamless authentication of credentials from multiple agencies at the local, state, and federal levels. This function would prove invaluable during an emergency situation. Multi-jurisdictional electronic validation for first responders has been one benefit of the implementation of PKI in the state of Illinois. Using this system, Illinois first responders will be allowed quick access to disaster sites. Because the Illinois credentials are in compliance with the Department of Homeland Security guidelines, it is expected that the credentials would be accepted nationally should any Illinois first responders volunteer to assist in other jurisdictions (Identity, Credential and Access Management Sub Committee, 2010).
- OAKS Financials- Vendors
    - New and existing vendors must submit forms to add and/or change their information in the state's vendor database. The forms are available online, but require a wet signature when submitted. If electronic signatures were implemented, the form could be fully completed online. This would save the vendors time and money, and it could potentially reduce errors in form completion.
- SOS Business Licensing
    - Currently the Secretary of State's Office requires that business filing forms must include a signature in order to be processed. Electronic signatures could simplify this procedure and allow for faster processing and response.
- Licensing
    - Ohio Department of Natural Resources (ODNR) – Electronic signatures could benefit ODNR in its administration of hunting and fishing licenses. Current purchase procedures include the following steps: (1) customer identification, (2) product selection, (3) payment, and (4) print and sign your licenses and permits.
- Electronic Rule Filing (ORC 119.04)
    - When an administrative rule is final filed using the Electronic Rule Filing (ERF) System, an agency director must enter a PIN to complete the filing. The PIN takes the place of the Director's signature on paper copies of rules. Its use

certifies that the electronically filed rules are true and accurate copies of the rules adopted by the Director's agency.

- Department of Taxation
  - The Ohio Department of Taxation implemented a form of electronic signature as part of the Ohio TeleFile system. When a taxpayer submits a tax return via telephone, the user is asked to enter a unique taxpayer identification number (TIN) and is then required to enter another number to acknowledge and submit the contents of the tax return.
- Internal state processes
  - Closer inspection of internal state processes will likely result in the identification of additional workflows that would benefit from electronic signature technology.

In order for Ohio to be competitive in the global market, the state must establish an infrastructure that supports digital signatures and paperless processes. This paper has examined the technology, legal environment, and use of digital signatures in Ohio and other states. It recommends that Ohio update its current policies in light of today's security threats and business opportunities. The existing administrative rule governing the use of electronic signatures has not been updated since 2007 and should be reviewed, particularly to determine whether it needs to be amended to eliminate unnecessary paperwork (ORC section 119.032(C)(3)). This paper proposes that a governance group be created to oversee the policies, decision-making, and implementation efforts necessary to establish a PKI for use within the state. It also recommends that the state incorporate the requirements necessary to tie into similar efforts at the federal level (FPKI). Finally, it recommends that the state should actively review the systems accessed through the Ohio Business Gateway to determine if digital signature technology is appropriate.

References

Bakolia, G. (2009). *Electronic document management and digital signatures for North Carolina state government*. Retrieved from https://www.scio.nc.gov/library/pdf/Document_Management_Report.pdf

Department of Commerce. (2001). *Electronic signatures in global and national commerce act.* Retrieved from http://www.ftc.gov/os/2001/06/esign7.htm

Dictionary.com unabridged. (n.d). *Signature*. Retrieved from http://dictionary.reference.com/browse/signature

Entrust. (2003). *Digital signatures—best practice for e-business transactions*. Retrieved from http://download.entrust.com/resources/download.cfm/21155/

Entrust. (2009). *3 elements that comprise a high quality PKI…and how you can get it for less*. Retrieved from www.entrust.ca/resources/download.cfm/23676

[FIPS 186-3] National Institute of Standards and Technology Federal Information Processing Standards FIPS 186-3, Digital Signature Standard (DSS), June 2009.

[HISBEsign2001] American National standards Institute Health Care Informatics Standards Board (ANSI HISB) March 2001.

Lantsman, B. (n.d.). *Think twice before you sign anything again: 12 business cases for digital signatures.* (n.d). Retrieved from http://www.arx.com/files/DOCUMENTS/Digital-signature-eBook.pdf

Identity, Credential and Access Management Sub Committee (ICAMSC). (2010). *The realized value of the Federal public key infrastructure (FPKI).* Retrieved from www.idmanagement.gov/documents/RealizedValueFederalPKI.pdf

Identrust. (n.d). *Aces certificates*. Retrieved from http://www.identrust.com/agency/aces.html

Identrust. (2009). *State of Virginia adopts ACES.* Retrieved from http://www.identrust.com/company/press_releases/2009/release_091005.pdf

McLaughlin, L. (2001, September 1). Identity crisis: pfizer's fix. *CIO*, *20*(22), 47-50.

National Conference of Commissioners on Uniform State Laws. (2010). *Electronic transactions act*. Retrieved from http://www.nccusl.org/Act.aspx?title=Electronic%20Transactions%20Act

[NIST IR 7298 Rev1] National Institute of Standards and Technology Interagency Report Revision 1, Glossary of Key Information Security Terms, February 2011.

[NIST IR 7313] National Institute of Standards and Technology Interagency Report, 5th Annual PKI R&D Workshop “Making PKI Easy to Use” Proceedings, July 2006.

[NIST IR 7581] National Institute of Standards and Technology Interagency Report 7581, System and Network Security Acronyms and Abbreviations, September 2009.

[NIST SP 800-32] National Institute of Standards and Technology , Introduction to Public Key Technology and the Federal PKI Infrastructure, February 2001.

[NIST SP 800-35] National Institute of Standards and Technology SP 800-35, Guide to Information Technology Security Services, October 2003.

[NIST SP 800-63] National Institute of Standards and Technology SP 800-63, Electronic Authentication Guideline, April 2006.

Ohio Department of Administrative Services, Office of Statewide IT Policy. (2004). *Public key infrastructure: proposed enterprise strategy for the state of Ohio (strategy 0.2.1)*. Columbus, OH.

Rohatgi, A. (2008*). Implementation of the 'digital signatures' in the state government agencies of the Commonwealth of Virginia.* Virginia Enterprise Applications Program. Retrieved from http://www.virginiadot.org/business/resources/LocDes/Digital_Signature_Initiative_071508.pdf

State of Ohio. (2011). *2011 state of the state address*. Retrieved from http://governor.ohio.gov/LinkClick.aspx?fileticket=FOdznJHdKRE%3d&tabid=40

US Department of Homeland Security. (2011). Homeland security presidential directive 12: Policy for a common identification standard for federal employees and contractors. Retrieved from HSPD-12 http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm#1

United States Office of Management and Budget. (n.d.). *Implementation of the government paperwork elimination act.* Retrieved from http://www.whitehouse.gov/omb/fedreg_gpea2/

Washington Secretary of State. (n.d.). *Glossary of digital signature terms.* Retrieved from http://www.sos.wa.gov/ea/overview_glossary.aspx

Appendix A: Glossary of Terms

Acronyms and Abbreviations (includes excerpts from NIST 800-32)

ACES	Access Certificates for Electronic Services
CA	Certification Authority
CHRI	Criminal History Record Information
CIO	Chief Information Officer
DMME	Department of Mines and Minerals and Energy (Virginia)
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECA	External Certification Authority
ERC	Enhanced Reliability Check
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FBCA OA	Federal Bridge Certification Authority Operational Authority
FED-STD	Federal Standard
FIPS PUB	Federal Information Processing Standard Publication
FPKISC	Federal PKI Steering Committee
FPKIPA	Federal PKI Policy Authority
FTS	Federal Technology Service
GITSB	Government Information Technology Services Board
GPEA	Government Paperwork Elimination Act of 1998
GSA	General Services Administration
HIPAA	Health Insurance Portability and Accountability Act of 1996
ISAC	Illinois Student Assistance Commission
ISO	International Organization for Standardization
ITL	Information Technology Laboratory
MOA	Memorandum of Agreement
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OAC	Ohio Administrative Code
OAKS	Ohio Administrative Knowledge System
OID	Object Identifier
OIT	Office of Information Technology (State of Ohio)
ORC	Ohio Revised Code
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman
SHA-1	Secure Hash Algorithm, Version 1
SHA-256	Secure Hash Algorithm (256 bits)
SOS	Secretary of State
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
U.S.C.	United States Code
WWW	World Wide Web

Definitions and Terms (includes excerpts from NIST 800-32)

Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Agency CA	A CA that acts on behalf of an Agency, and is under the operational control of an Agency.
Attribute Authority	An entity, recognized by the Federal PKI Policy Authority or comparable Agency body as having the authority to verify the association of attributes to an identity.
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. (NIST) Assurance that the electronic signature is that of the person purporting to sign a record or otherwise conducting an electronic transaction (Ohio Administrative Code Rule 123:3-1-01).
Biometric	A physical or behavioral characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs.
Certification Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certificate Status Authority	A trusted entity that provides online verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.

Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Cross-Certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Cryptography	A branch of applied mathematics concerned with transformations of data for security purposes.
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	An encrypted electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature. (ORC 1733.29(H)(2)(d)) The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made. (NIST 800-32)
Digitized Signature	A graphical image of a handwritten signature, generally created by scanning in a handwritten signature.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Electronic Signature	ORC section 1306.01(H) defines electronic signature as "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." On the federal level, The Government Paperwork Elimination Act defines it as any method of signing an electronic message that identifies and authenticates the person who is the source of the message and indicates their approval of the contents (NIST 800-32).
Electronic Transaction	The exchange of an electronic record and electronic signature between a state agency and a person to: consent to release information; purchase, sell, or lease goods, services or construction; transfer funds; facilitate the submission of an electronic record with an electronic signature required or accepted by a state agency; or create records upon which the State of Ohio or any other person will reasonably rely including but not limited to formal communication, letters, notices, directives, policies, guidelines and any other record (OAC rule 123:3-1-01).
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
Federal Bridge Certification Authority (FBCA)	The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer-to-peer interoperability among Agency Principal Certification Authorities.

Federal Bridge Certification Authority Membrane	The Federal Bridge Certification Authority Membrane consists of a collection of Public Key Infrastructure components including a variety of Certification Authority PKI products, Databases, CA specific Directories, Border Directory, Firewalls, Routers, Randomizers, etc.
FBCA Operational Authority	The Federal Bridge Certification Authority Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.
Federal Public Key Infrastructure Policy Authority (FPKI PA)	The Federal PKI Policy Authority is a federal government body responsible for setting, implementing, and administering policy decisions regarding interagency PKI interoperability that uses the FBCA.
Integrity	Protection against unauthorized modification or destruction of information. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Memorandum of Agreement (MOA)	Agreement between the Federal PKI Policy Authority and an Agency allowing interoperability between the Agency Principal CA and the FBCA.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the four policies and cryptographic algorithms supported.

Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the Federal PKI Policy Authority.
Principal CA	The Principal CA is a CA designated by an Agency to interoperate with the FBCA. An Agency may designate multiple Principal CAs to interoperate with the FBCA.
Privacy	Restricting access to subscriber or Relying Party information in accordance with Federal law and Agency policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Signature	A person's name or a mark representing it, as signed personally or by deputy, as in subscribing a letter or other document.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Smart Card	A credit card-sized card with embedded integrated circuits that can store, process, and communicate information. (NIST IR-7298)
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of an Agency in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor."
Wet Signature	A traditional handwritten signature generally applied to a paper document. Often used interchangeably with the term "Signature."

Selected Bibliography

[NIST SP 800-35] National Institute of Standards and Technology SP 800-35, Guide to Information Technology Security Services, October 2003.

[HISBEsign2001] American National standards Institute Health Care Informatics Standards Board (ANSI HISB) March 2001.

[NIST IR 7298 Rev1] National Institute of Standards and Technology Interagency Report Revision 1, Glossary of Key Information Security Terms, February 2011.

[FIPS 186-3] National Institute of Standards and Technology Federal Information Processing Standards FIPS 186-3, Digital Signature Standard (DSS), June 2009.

[NIST IR 7313] National Institute of Standards and Technology Interagency Report, 5th Annual PKI R&D Workshop "Making PKI Easy to Use" Proceedings, July 2006.

[NIST SP 800-32] National Institute of Standards and Technology , Introduction to Public Key Technology and the Federal PKI Infrastructure, February 2001.

[NIST SP 800-63] National Institute of Standards and Technology SP 800-63, Electronic Authentication Guideline, April 2006.

[NIST IR 7581] National Institute of Standards and Technology Interagency Report 7581, System and Network Security Acronyms and Abbreviations, September 2009.

Appendix B: List of state agencies that submitted an Electronic Transaction Report to DAS-OIT pursuant to Ohio Administrative Code rule 123:3-1-01

1. Administrative Services

a. Ohio Business Gateway
b. Record Information Management System (RIMS)
c. OIT Vendor Contracts

2. Budget and Management

a. eControlling Board

3. Commerce

a. Agency Store EFT
b. Appraisal Registry Data Transfer
c. Central Registration Depository
d. E-mail receipt of address change
e. Migrant Inspection Surveys
f. Minor Work Permit
g. Needlestick Device Registration
h. Needlestick Incident Reporting
i. OASIS
j. Online Licensee File Look Up
k. OSHA Training Registration
l. OTTER
m. PERPP
n. Prevailing Wage
o. Union Contract

4. Consumers' Counsel

a. CAS Accounting and Payroll
b. Remote Access to OCC LAN
c. Remote Access to Research Databases

5. Cosmetology Board

a. Board Inspection Reports

6. Criminal Justice Services

a. Quarterly Subgrant Report ETR

7. Development

a. Ohio Investment in Training Program Application Signature Page

8. Industrial Commission

a. IC Hearing Orders Signature

9. Insurance

a. Producer Application Submission

10. Job & Family Services

a. Quarterly Payroll Reporting
b. Quarterly UC Contribution Payment
c. UC Benefit Transactions via OJI Claimant View
d. UC Benefit Transactions via OJI Employer View

11. Natural Resources

a. Boat Registration
b. Boating Education
c. File Transfers
d. Goods and services purchases, class and conference registration
e. General e-mail with public/staff/other governmental entities
f. Processing Ohio Boating Education Course (OBEC) online certificates
g. Recycle, Ohio! Grants Process
h. Time and Activity Reporting System (TARS)
i. Water Well Log Submittal

12. Public Safety

a. Crash Record Remote Access Module - Credit Card Payment
b. Intelligrants
c. OPlates

13. Taxation

a. 1040 Web Personal Income Tax Returns
b. ACH Payment Processing
c. CAT Registration
d. CVISN
e. E-File
f. International Fuel Tax Agreement
g. "Kilowatt Hours/Million Cubic Feet" – Electric Distributors (KWH) and Natural Gas Distributors (MCF) Tax Returns & Payments
h. Municipal Tax Electronic Forms
i. Monthly and Quarterly Income Tax Withholding Reporting using the Ohio Business Gateway (HB 202)
j. Pers IT Credit Card Pymnts
k. TeleFile IVR IT Return
l. Treasury Offset Program

14. Workers' Compensation

a. C108-Request for Waiver of Appeal
b. C-240 - Claim Settlement
c. Semiannual premium payment using the Ohio Business Gateway (HB 202)
d. C167-T-Permanent Partial Disability Compensation Objection
e. C60-Statement for Reimbursement of Travel Expense
f. C84-Request for Temporary Total Compensation
g. C141-Wage Loss Statement for Job Search

Appendix C: OAC 123:3-1-01 Transaction Risk Assessment

123:3-1-01 **Use of electronic signatures and records, office of information technology.**

(A) Definitions. In addition to the definitions in section 1306.01 of the Revised Code, the following definitions are also applicable to this rule:

(1) "Authentication" is the assurance that the electronic signature is that of the person purporting to sign a record or otherwise conducting an electronic transaction.

(2) "Domain" means category of persons based on the nature of the identity of the person.

(3) "Electronic transaction" means the exchange of an electronic record and electronic signature between a state agency and a person to:

(a) Consent to release information;

(b) Purchase, sell or lease goods, services or construction;

(c) Transfer funds;

(d) Facilitate the submission of an electronic record with an electronic signature required or accepted by a state agency; or

(e) Create records formally issued under a signature and upon which the state of Ohio or any other person will reasonably rely including but not limited to formal communication, letters, notices, directives, policies, guidelines and any other record. This subsection does not include informational publications and informal communications.

(4) "Integrity" is the assurance that the electronic record is not modified from what the signatory adopted.

(5) "Nonrepudiation" is the proof that the signatory adopted or assented to the electronic record or electronic transaction.

(6) "Office of Information Technology" (OIT) is the entity housed within the department of administrative services under section 125.18 of the Revised Code to provide state governance and direction for information technology.

(B) Scope.

(1) This rule applies only to electronic transactions involving a state agency. In accordance with section 1306.20 of the Revised Code, for the purposes of this section, "state agency" means every organized body, office, or agency established by the laws of the state for the exercise of any function of state government, but does not include the general assembly, any legislative agency, the supreme court, the other courts of record in this state, or any judicial agency.

(2) This rule applies to electronic transactions that include electronically signed records or electronic transactions involving a monetary transfer between a state agency and an individual, a corporation or another entity.

(C) General rule.

(1) Electronic transactions have the equivalent level of legal protection that is given to paper-based transactions. All security procedures and technologies should provide authentication, nonrepudiation and integrity to the extent that is reasonable for each electronic transaction.

(2) This rule establishes an overarching security procedure that requires state agencies to:

(a) Document uses of electronic transactions;

(b) Conduct a transaction risk assessment of each set of similar electronic transactions;

(c) Use, as a minimum, technology standards and/or security procedures that are appropriate for the level of transaction risk as determined by the security assessment;

(d) Establish and maintain documented security policies and procedures;

(e) Seek a waiver from OIT if the state agency determines that the security technologies or procedures do not conform to the minimum technology standards as established by this rule for the level of security identified in the transaction risk assessment.

(D) Documenting uses of electronic transactions.

(1) For each set of similar electronic transactions, state agencies must complete an electronic transaction report before acquiring or implementing electronic signatures, transactions or related technology. Agencies must complete and update electronic transaction reports on forms provided by OIT at http://www.ohio.gov/itp. Agencies must maintain electronic transaction reports for as long as the electronic records of the electronic transaction are retained in accordance with that agency's record retention schedule.

(2) Each electronic transaction report must include:

(a) The identification and description of the set of similar electronic transactions;

(b) The domain under which the electronic transaction set falls;

(c) A transaction risk assessment that identifies the potential impact of a security breach and the probability of attempts to breach security;

(d) A determination of the security level required for the electronic transaction set per the transaction risk assessment;

(e) The security procedure used for the electronic transaction set; and

(f) A list of documented agency security policies for physical, network and computer security. These documents must be clearly referenced and maintained on file and available for audit.

(3) State agencies must update electronic transaction reports to accurately reflect changes in the electronic transaction's associated risk, technology or security procedures. If the state agency determines that due to these changes in risk, technology or security procedures, the electronic transaction does not conform to the minimum technology standard for the level of security identified in the transaction risk assessment, the state agency must modify the risk, technologies or procedures to bring the electronic transaction into compliance with this rule or the state agency shall seek a waiver from OIT.

(E) Electronic transaction domains. Persons using electronic transactions in the course of government affairs fall in one of three domains - the citizen domain, the business domain or the state internal domain.

(1) Citizen domain: The citizen domain consists of individuals acting on their own behalf or on the behalf of any other individual under a power of attorney. The citizen domain includes only those individuals who choose to interact electronically with the state of Ohio. The citizen domain also includes state Web and application servers that interact with citizens.

(2) Business domain: The business domain consists of corporations, business trusts, partnerships, limited liability companies, associations, joint ventures or any other commercial, charitable or legal entity that interacts electronically with state agencies. This domain also includes Web and application servers that interact with businesses.

(3) State internal domain: The state internal domain consists of state employees acting on behalf of the state, and any other agent of the state; network components; and web and application servers that use electronic transaction-enabled applications to conduct internal state business. The state internal domain also applies to local government representatives for electronic transactions with state government agencies.

(F) Transaction risk assessment.

(1) As part of the agency report, agencies must complete an assessment of the transaction risk for the use of the set of similar electronic transactions. The transaction risk assessment identifies the appropriate security level by analyzing the impact of a security breach and the probability of attempt to breach security.

(2) In determining the potential impact of a security breach, state agencies shall consider the:

(a) Intended use of the electronic record or signature;

(b) Type of information being transmitted, received or stored;

(c) Network used;

(d) Degree of risk to the state;

(e) Degree of risk to the users of the system;

(f) Degree of risk to third parties;

(g) Projected volume of transactions;

(h) Estimated cost;

(i) Potential legal liability; and

(j) Appropriate requirements for authentication of identity.

(3) Impact of a security breach. The potential impact of a security breach falls into one of four categories - low-impact, medium-impact, high-impact and very high-impact.

(a) Low-impact: A security breach is considered low-impact if there is no impact of a breach of security or the impact is slight or so insignificant that there would be no or only a slight and negligible financial loss, loss of the public's trust or adverse legal consequences.

(b) Medium-impact: A security breach is considered medium-impact if the impact is limited in nature. Limited in nature means that: (i) the financial loss when averaged for the electronic transaction set is less than ten thousand dollars to the business, citizen, state or other entity involved, (ii) there are no major adverse legal implications or (iii) the breach would cause at least some but not significant public distrust of the state.

(c) High-impact: A security breach is considered high-impact if: (i) compromised security would have a significant impact so that the financial harm when averaged for the electronic transaction set ranges from ten thousand dollars to five hundred thousand dollars, or (ii) the breach would result in media scrutiny and significant public distrust, or (iii) the breach would have adverse legal consequences.

(d) Very high-impact: The result of a security breach that has a very high impact would be extremely serious. This type of breach results in: (i) the financial loss, when averaged for the electronic transaction set, exceeding five hundred thousand dollars, or (ii) considerable legal violations, or (iii) intense media scrutiny and widespread, deep public distrust.

(4) Probability of an attempt to breach security. The primary consideration is the value of a security breach to a person attempting a breach. Value includes financial gain, unauthorized access to confidential information and the ability to harass, embarrass or shock. The probability is characterized as low, medium or high.

(a) Low-probability: A low-probability electronic transaction is one that would have little value to someone attempting a breach, and therefore, the likelihood of

breach attempts is small with any attempts likely to be none or few and limited in effort.

(b) Medium-probability: A medium-probability electronic transaction is one which would provide value to someone seeking to breach security.

(c) High-probability: A high-probability electronic transaction would provide great value to someone should he or she breach security.

(5) Transaction risk assessment. The transaction risk assessment results in a determination that the electronic transaction falls within one of four minimum security levels - low (level A), medium (level B), high (level C) or very high (level D). The minimum security level is determined by the combination of the level of the impact of a security breach and the level of probability of a security breach as identified in the following table:

Transaction risk assessment as determined by the impact of a security breach and the probability of a security breach

	Low-probability	Medium-probability	High-probability
Low-impact	Level A	Level A	Level B
Medium-impact	Level B	Level B	Level B
High-impact	Level B	Level C	Level C
Very high-impact	Level C	Level C	Level D

(G) Security procedures appropriate for security levels. Each electronic transaction set must conform to the minimum security procedures including technology standards for the level of security identified in the transaction risk assessment. State agencies may choose to meet the requirements of higher security levels with level A being least secure and level D being the most secure.

(1) For any transaction used at levels B, C, or D or any level A transaction involving confidential data or a monetary transfer, the transmission of user-IDs and passwords must be encrypted using secure sockets layer or equivalent encryption when transmitted over the Internet.

(2) Level A: Under this level of security, state agencies may use any technological means for processing these sets of electronic transactions and providing assurance of authentication, nonrepudiation and integrity. State agencies shall document level A electronic transaction sets per paragraph (D)(1) of this rule.

(3) Level B: Level B electronic transactions must use at a minimum one of the following two security procedures for authentication: (a) a unique user-ID and an alphanumeric password consisting of at least eight characters, or (b) a smartcard or physical device with a unique proprietary password as an alternative. State agencies documenting level B electronic transaction sets per paragraph (D)(1) of this rule must describe in the electronic transaction report the authentication process including information of the initial registration process and the means used to prove the identity of persons registering to use electronic transactions.

(4) Level C: Under level C security, state agencies must submit the electronic transaction report to OIT and shall not use the electronic transaction until OIT approves the electronic transaction as being in compliance with this rule. State agencies must use digital certificates subject to paragraph (G)(4)(a) of this rule for these electronic transaction sets or the alternative in paragraph (G)(4)(b) of this rule.

(a) Digital certificates used for electronic signatures require a significant infrastructure known as public key infrastructure (PKI). Therefore, state agencies may use a PKI only with the approval of OIT. Pursuant to section 1306.21 of the Revised Code, when OIT determines that a PKI implementation is feasible, OIT may require the use of a common PKI by state agencies.

(i) OIT may make a state PKI available for use by the general assembly, any legislative agency, local governments, the supreme court, the other courts of record in this state or any judicial agency. These agencies are not required to use a state PKI.

(ii) In establishing a PKI, OIT has the authority to review, approve and mandate components of a PKI including the registration process and authorities; certificate policies and certificate practices statements, certificate management including issuance, continued participation, certificate revocation and certificate suspension; and any other PKI policy, practice, management or operation. OIT may delegate any or all components of the PKI to state agencies or to vendors. OIT may revoke delegation of PKI components to a state agency or a vendor in the event that the state agency or vendor is in noncompliance with this rule, a certificate policy or any other PKI policy or agreement.

(iii) OIT or its delegatee may revoke the digital certificate of any person whose use of the digital certificate is not in conformance with this rule, a certificate policy or any other PKI policy or agreement.

(b) As an alternative to paragraph (G)(4)(a) of this rule, agencies may meet level C security by combining the use of a unique user-ID and an alphanumeric password consisting of at least eight characters with a smartcard or physical device. State agencies seeking approval of electronic transaction sets using this alternative must provide a description of the authentication process including information on the initial registration process and the means used to prove the identity of persons registering to use electronic transactions. OIT may require that state agencies use a common multi-agency smartcard or physical device infrastructure.

(5) Level D: For level D electronic transactions, state agencies must submit the electronic transaction report to OIT and shall not use the electronic transaction until OIT approves the electronic transaction as being in compliance with this rule. State agencies must use a digital certificate issued under a PKI approved by OIT in combination with a unique user-ID and an alphanumeric password consisting of at least eight characters and a smartcard or physical device or biometric. Like level C security, OIT may require state agencies use a common multi-agency infrastructure. Any state agency using a biometric must establish security policies to provide a high degree of assurance of the

integrity and, if applicable, confidentiality of the biometric information. Agencies subject to policies issued under section 125.18 of the Revised Code shall conform with any OIT policies and standards published at http://www.ohio.gov/itp for security, interoperability and need. While state agencies may use higher levels of security than required by the transaction risk assessment, for biometrics, a state agency seeking to implement the use of biometrics must provide a justification to OIT.

(H) Required policies. State agencies must establish documented policies and procedures that provide reasonable assurance of the authenticity of electronic signatures, the nonrepudiation of the records by the signatories and the integrity of the electronically signed records. This includes but is not limited to policies and procedures on access, control, monitoring, maintenance and any other actions necessary for physical, network and computer security. Nothing in this rule permits state agencies subject to policies under section 125.18 of the Revised Code to supersede or establish security policies in conflict with any of those policies which may be found at http://www.ohio.gov/itp.

(I) Interface requirements. When at any time during an electronic transaction a state agency requires a signature or is conducting a financial transaction, the state agency must require a separate and distinct action on the part of the person conducting the transaction for financial transactions and each signature. The separate and distinct action must be clearly marked as indicating an intent to complete a financial transaction or electronically sign a writing. The separate and distinct action may include a series of keystrokes, a click of a mouse or other similar action.

(J) Records retention requirements. State agencies' records retention practices must assure nonrepudiation, integrity and continued access to the electronic record.

(K) Waiver provisions. State agencies may request a waiver of this rule by OIT.

(1) Upon a state agency request for a waiver pursuant to paragraph (D) of this rule, the director of the OIT or the director's designee may waive the requirements of this rule for an electronic transaction set upon a showing by the state agency that the alternative security technology and procedures governing the set of similar electronic transactions do not compromise the level of security as determined by paragraphs (F) and (G) of this rule. Upon finding that the alternative security technologies or procedures are no longer appropriate for the level of risk, the OIT director may revoke the waiver.

(2) The waiver request is a letter to OIT identifying the electronic transaction set, stating that the state agency is seeking a waiver and providing a justification for the waiver. The request for waiver includes the electronic transaction report. The justification must show that the proposed alternative security technology and procedures provide authentication, nonrepudiation and integrity and do not compromise the level of security as determined by paragraphs (F) and (G) of this rule.

(L) Electronic transactions with agencies of other states and the federal government. This rule applies to electronic transactions between state agencies and federal agencies to the extent that it is consistent with federal law. OIT may coordinate the use of electronic signatures between state agencies and the federal government. OIT may coordinate the use of electronic signatures with agencies of another state.

Effective: 06/02/2007

R.C. 119.032 review dates: 04/03/2011
Promulgated Under: 111.15
Statutory Authority: 1306.21
Rule Amplifies: 1306.21
Prior Effective Dates: 12/22/2000, 04/03/2006

Electronic Transaction Report

In accordance with rule 123:3–1–01 of the Administrative Code and Executive Order 2004-02T, please complete this report. Electronic transactions falling within levels C and D must be submitted to:

DAS-OIT USE
Date Received:

Enterprise IT Architecture and Policy
Investment and Governance Division
Office of Information Technology
30 E. Broad Street, 39th Floor
Columbus, OH 43215
Voice: 614-752-7204
Fax: 614-644-9152
Email: OITLawAndPolicyAdvisor@oit.ohio.gov.

1. Agency	**2. Date**
3. Electronic Transaction (short name)	
4. Contact Name: Title: Email: Phone: Address:	

5. Project Status (check one)

- o Initial planning stages
- o Plan developed
- o Preparing acquisition of technology or service
- o Implementing technology or service
- o Electronic transactions are in place

6. Requesting (check one)

- o Approval
- o Waiver

7. Description

Briefly describe the proposed set of similar electronic transactions in the context of the use of the legally binding electronic record or signature, the objects and nature of the exchange, the technology and security procedures used to assure authentication (the technology and process including the initial registration process used to assure the identity of person purporting to sign the record), integrity (the technology and the process used to assure that the records have not been changed and can be accessed for as long as the law demands) and nonrepudiation (the technology and process used to associate the electronic signature with the record).

8. Domain (check one) o Internal State o Business o Citizen See subsection (E) of rule 123:3-1-01 of the Administrative Code. Please briefly describe the person (individual, business, government employee, etc.) who will be using the electronic transaction with your state agency.
9. Security Assessment See subsection (F) of rule 123:3-1-01 of the Administrative Code. The security assessment identifies the potential **impact** of a security breach and the **probability** of such a breach occurring. Indicate the level of impact and risk for the particular set of similar electronic transactions and provide a brief narrative explaining how the levels were selected. Then determine the required **security level** as established in the matrix provided in the rule.

Impact	A. Please identify the impact of a security breach (check one): o Low o Medium o High o Very High Provide a brief narrative applying the criteria of paragraphs (F)(2-3) of rule 123:3-1-01 of the Administrative Code. Please note that the financial thresholds that are listed in paragraph (F)(3) reference the *average* financial impact for the individual transactions that make up the proposed set of similar electronic transactions.

Risk	B. Please identify the probability or likelihood of someone attempting a security breach in order to obtain something of value such as financial gain, unauthorized access to confidential information, or the ability to harass, embarrass or shock. (check one): o Low o Medium o High Provide a brief narrative applying the criteria of paragraph (F)(4) of rule 123:3-1-01 of the Administrative Code.
Security Level	C. Please identify the security level required for the proposed set of similar electronic transactions as determined by the matrix provided in paragraph (F)(5) of rule 123:3-1-01 of the Administrative Code. o Level A o Level B o Level C o Level D

10. Technologies and Security Procedures Summary

Please identify the technology (including hardware and software under consideration and please specify versions or software levels) and security procedure(s) used for the proposed set of similar electronic transactions (check one):

o Approval:

Specifically explain in an attachment how the proposed technologies and security procedures meet the minimum requirements as identified in paragraph (G) of rule 123:3-1-01 of the Administrative Code. Also, provide information on additional technologies and security procedures that affect the level of assurance of authentication, integrity and nonrepudiation. These additional procedures might include but are not limited to out of band communications (e.g., confirmation sent through standard mail), identity proofing procedures (e.g., initial personal appearance or cross-checking information against multiple databases), additional password rules (e.g. lockout rules, periodic required password changes, etc.), the use of shared secrets or other procedures that increase (or decrease) security and comprehensive database access controls ranging from users to developers.

o Waiver:

Provide the information required by paragraph (K) of rule 123:3-1-01. Specifically explain in an attachment how the proposed technologies and security procedures are equivalent to the minimum requirements as identified in paragraphs (F) and (G) of rule 123:3-1-01 of the Administrative Code (establishing the appropriate level of assurance of authentication including the initial registration process, integrity and nonrepudiation). These technologies and security procedures might include secure technologies not identified in the rule, out of band communications (e.g., confirmation sent through standard mail), multiple database checks, password rules (e.g. lockout rules, periodic required password changes, etc.) or other procedures that increase (or decrease) security. Please attach a justification as to why the rule should not apply to the proposed set of similar electronic transactions and why the requirements of the rule should be waived.

11. Security Policies

Please provide a list (including title and date) of documented agency security policies for physical, network and computer security as related to this electronic transaction set. These documents must be clearly referenced, maintained on file and available for audit.

12. Justification for Use of Biometrics

If the electronic transaction uses a biometric, provide a justification as an attachment for the use of the biometric.

13. Definitions

Transaction

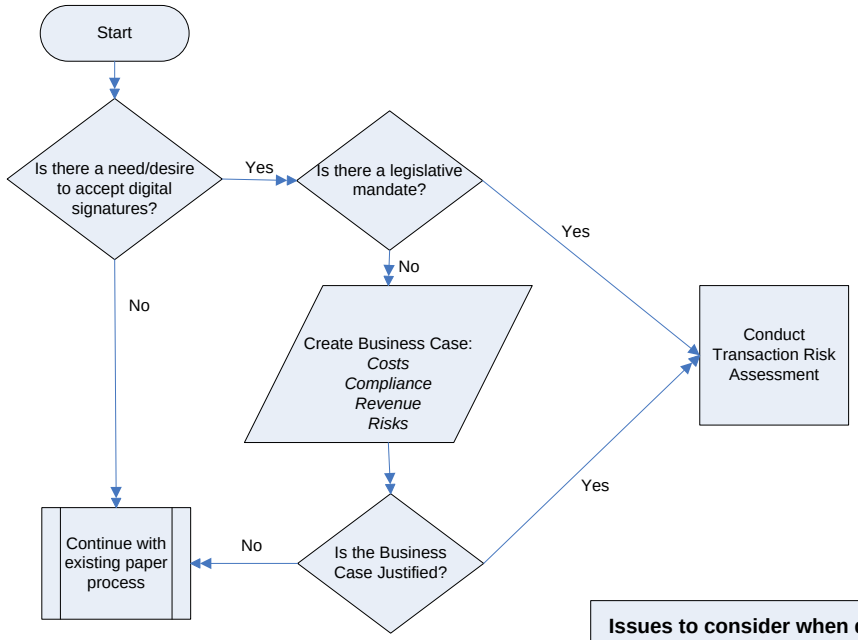
The definition of “transaction” under UETA is “an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs” (section 1306.01 of the Revised Code). In the state government context, this covers transactions between a government agency and citizens, business and other government agencies and includes not only financial exchanges but also filings, registrations, etc. The term does not carry the meaning that is often used in the technical field of a change or update to a database.

Electronic Records

The term “electronic records” as referenced in UETA does not carry the same definition or application as the term “public record” as defined in ORC 149.43. The electronic records that UETA references are much fewer in number than the number of public records that are kept in electronic formats. UETA and the subsequent administrative rule apply only to electronic records that relate to an electronic transaction (section 1306.02 of the Revised Code). Furthermore, the application of UETA for use of electronic records and signatures by state agencies should not be read outside of the context of section 1306.06 (or most of chapter 1306) of the Revised Code. Therefore, the requirements of UETA and the administrative rule only apply to records (in electronic format) that either the law requires to be in writing or that agencies want to have a legal effect. Public records under ORC 149.43 are “any record that is kept by any public office” and not excepted by ORC 149.43. This definition is very broad and includes records beyond the scope of UETA. The fact that a public record is in an electronic format alone is not enough to make it fall within chapter 1306 of the Revised Code.

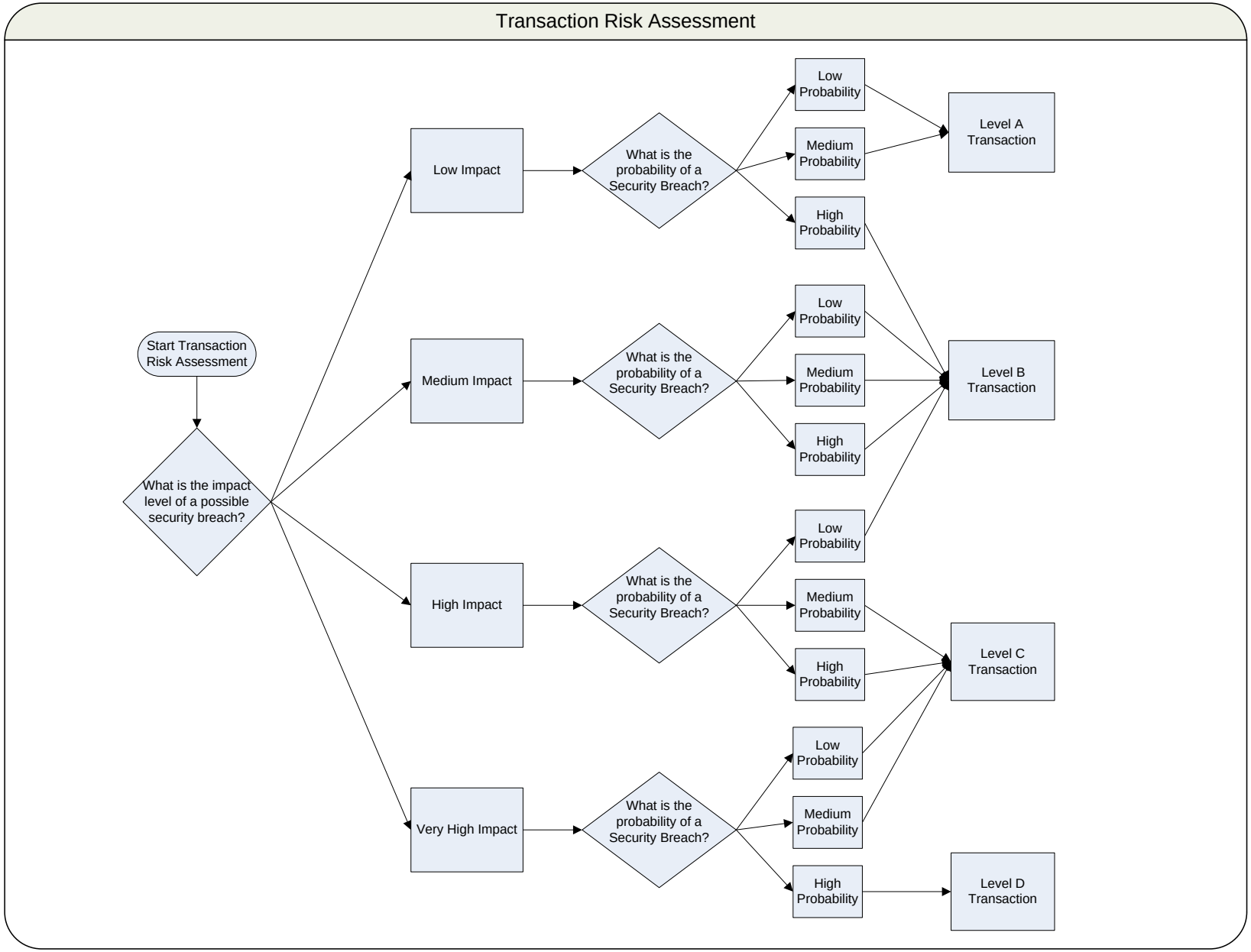
Appendix E: Transaction Risk Decision Matrix

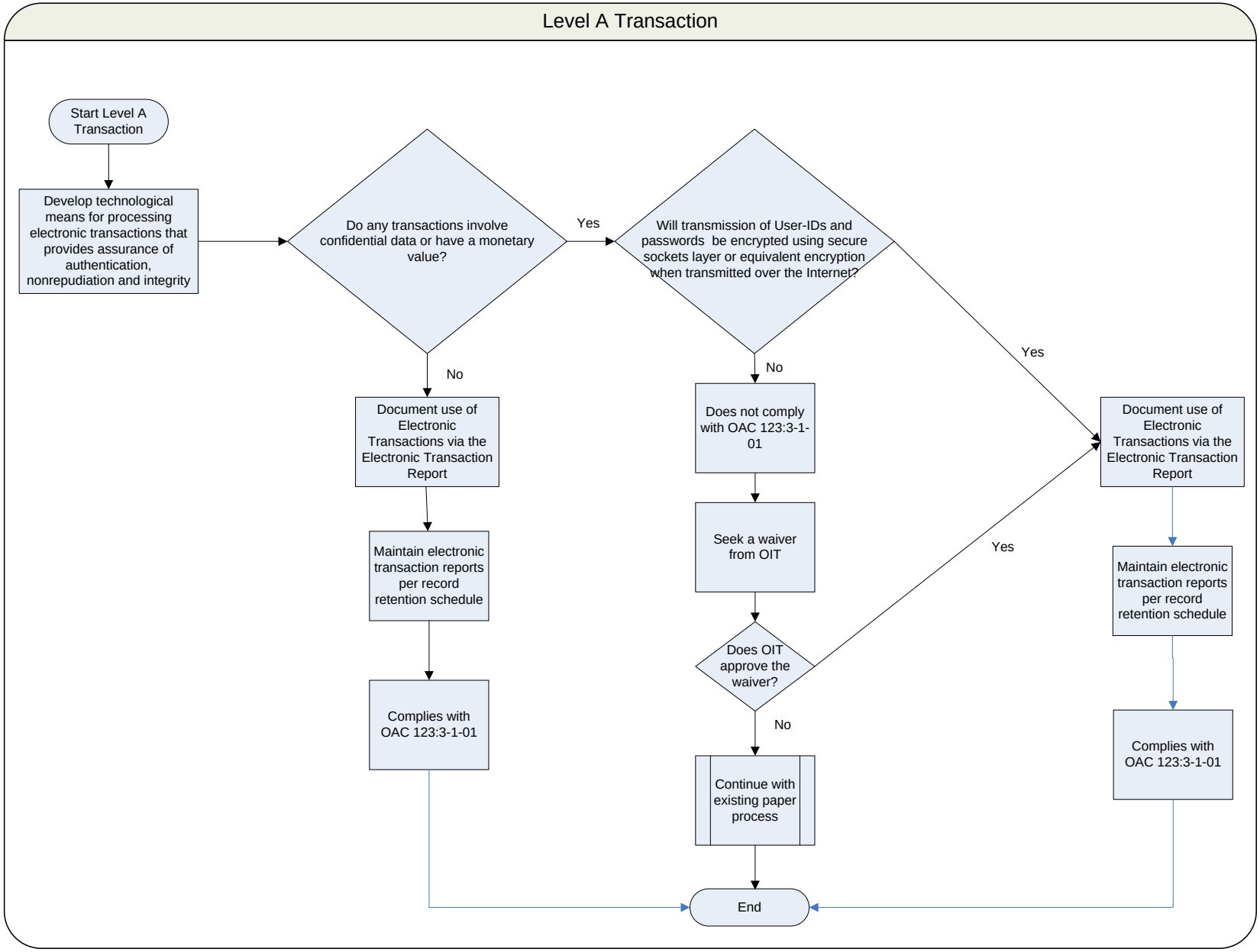
Digital Signature Decision Model

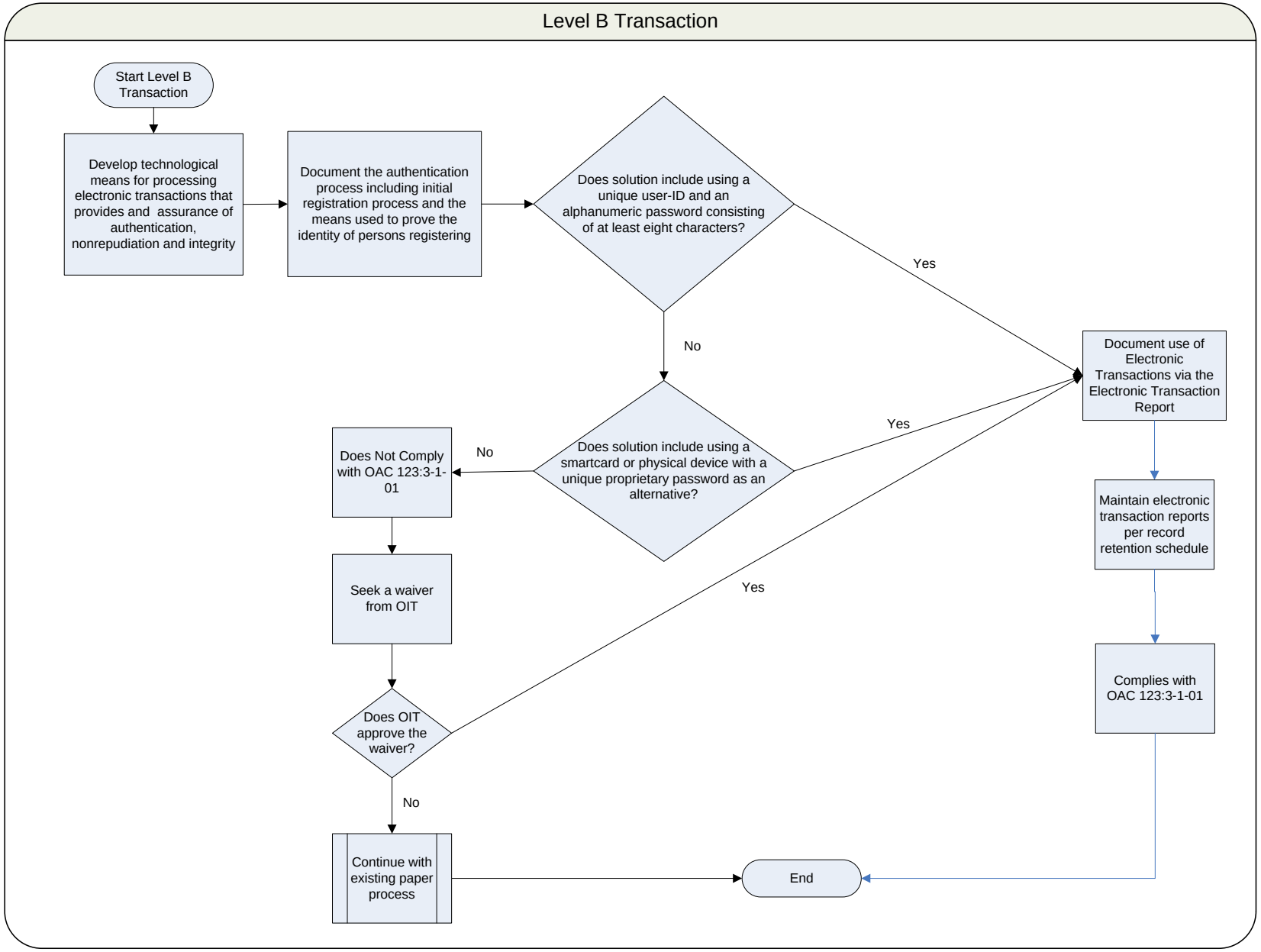


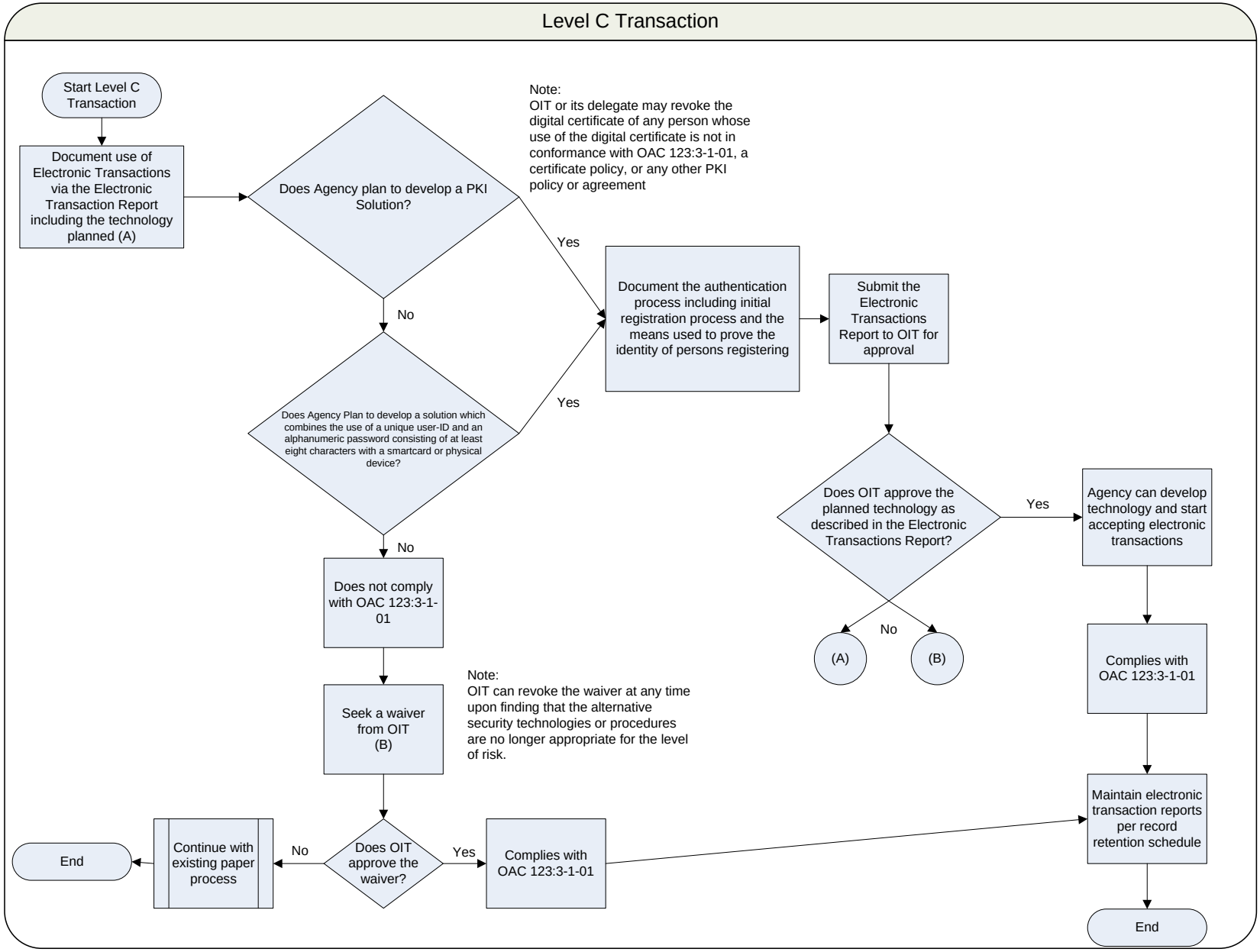
Issues to consider when deciding to accept the amount of security necessary to conduct a transaction:

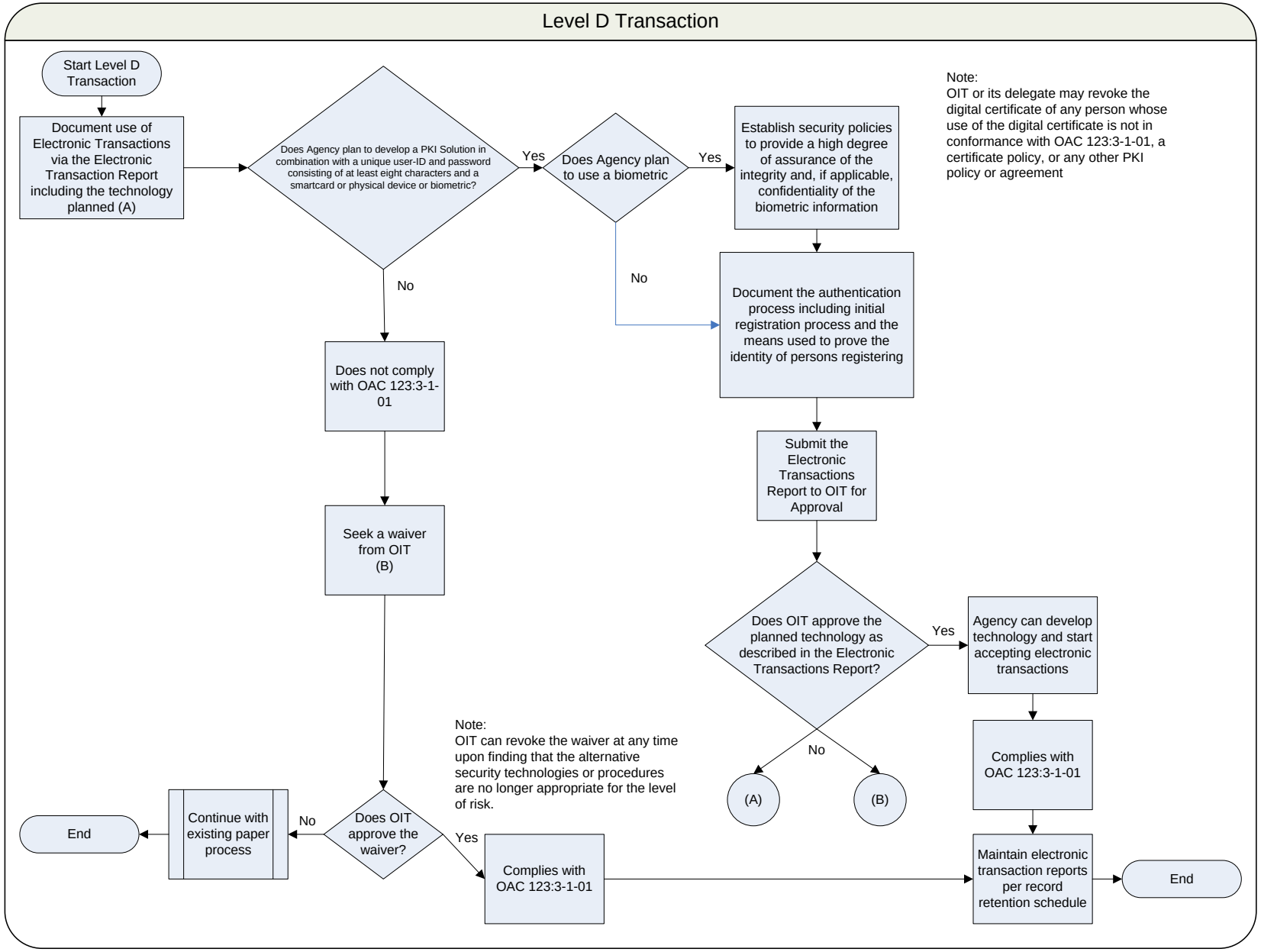
- Does the signature on the document need to be verified?
- How much time and resources can be allocated to verification?
- Does the signature need to be compared to a manual signature on paper or can a digital certificate adequately provide one-stop verification?
- Will immediate verifiability reduce the potential of fraud?
- Will the documents containing digital signatures need to be reproduced for public access to the records?
- Will the documents containing digital signatures need to be utilized by another local, state or federal agency? If so, is the technology compatible with other agency's needs?


Transaction Risk Assessment
Start Transaction Risk Assessment
What is the impact level of a possible security breach?
Low Impact
Medium Impact
High Impact
Very High Impact
What is the probability of a Security Breach?
What is the probability of a Security Breach?
What is the probability of a Security Breach?
What is the probability of a Security Breach?
Low Probability
Medium Probability
High Probability
Low Probability
Medium Probability
High Probability
Low Probability
Medium Probability
High Probability
Low Probability
Medium Probability
High Probability
Level A Transaction
Level B Transaction
Level C Transaction
Level D Transaction


Level A Transaction
Start Level A Transaction
Develop technological means for processing electronic transactions that provides assurance of authentication, nonrepudiation and integrity
Do any transactions involve confidential data or have a monetary value?
Yes
No
Will transmission of User-IDs and passwords be encrypted using secure sockets layer or equivalent encryption when transmitted over the Internet?
No
Yes
Document use of Electronic Transactions via the Electronic Transaction Report
Maintain electronic transaction reports per record retention schedule
Complies with OAC 123:3-1-01
Does not comply with OAC 123:3-1-01
Seek a waiver from OIT
Does OIT approve the waiver?
Yes
No
Continue with existing paper process
Document use of Electronic Transactions via the Electronic Transaction Report
Maintain electronic transaction reports per record retention schedule
Complies with OAC 123:3-1-01
End


Level B Transaction
Start Level B Transaction
Develop technological means for processing electronic transactions that provides and assurance of authentication, nonrepudiation and integrity
Document the authentication process including initial registration process and the means used to prove the identity of persons registering
Does solution include using a unique user-ID and an alphanumeric password consisting of at least eight characters?
Yes
No
Does solution include using a smartcard or physical device with a unique proprietary password as an alternative?
No
Yes
Does Not Comply with OAC 123:3-1-01
Seek a waiver from OIT
Does OIT approve the waiver?
Yes
No
Continue with existing paper process
Document use of Electronic Transactions via the Electronic Transaction Report
Maintain electronic transaction reports per record retention schedule
Complies with OAC 123:3-1-01
End


Level C Transaction
Start Level C Transaction
Document use of Electronic Transactions via the Electronic Transaction Report including the technology planned (A)
Does Agency plan to develop a PKI Solution?
Note:
OIT or its delegate may revoke the digital certificate of any person whose use of the digital certificate is not in conformance with OAC 123:3-1-01, a certificate policy, or any other PKI policy or agreement
Yes
No
Document the authentication process including initial registration process and the means used to prove the identity of persons registering
Submit the Electronic Transactions Report to OIT for approval
Does Agency Plan to develop a solution which combines the use of a unique user-ID and an alphanumeric password consisting of at least eight characters with a smartcard or physical device?
Yes
No
Does OIT approve the planned technology as described in the Electronic Transactions Report?
Yes
No
(A)
(B)
Agency can develop technology and start accepting electronic transactions
Complies with OAC 123:3-1-01
Does not comply with OAC 123:3-1-01
Seek a waiver from OIT (B)
Note:
OIT can revoke the waiver at any time upon finding that the alternative security technologies or procedures are no longer appropriate for the level of risk.
Does OIT approve the waiver?
No
Yes
Continue with existing paper process
End
Complies with OAC 123:3-1-01
Maintain electronic transaction reports per record retention schedule
End


Level D Transaction
Start Level D Transaction
Document use of Electronic Transactions via the Electronic Transaction Report including the technology planned (A)
Does Agency plan to develop a PKI Solution in combination with a unique user-ID and password consisting of at least eight characters and a smartcard or physical device or biometric?
Yes
Does Agency plan to use a biometric
Yes
Establish security policies to provide a high degree of assurance of the integrity and, if applicable, confidentiality of the biometric information
Note:
OIT or its delegate may revoke the digital certificate of any person whose use of the digital certificate is not in conformance with OAC 123:3-1-01, a certificate policy, or any other PKI policy or agreement
No
No
Document the authentication process including initial registration process and the means used to prove the identity of persons registering
Does not comply with OAC 123:3-1-01
Submit the Electronic Transactions Report to OIT for Approval
Seek a waiver from OIT (B)
Does OIT approve the planned technology as described in the Electronic Transactions Report?
Yes
Agency can develop technology and start accepting electronic transactions
No
(A)
(B)
Complies with OAC 123:3-1-01
Note:
OIT can revoke the waiver at any time upon finding that the alternative security technologies or procedures are no longer appropriate for the level of risk.
End
Continue with existing paper process
No
Does OIT approve the waiver?
Yes
Complies with OAC 123:3-1-01
Maintain electronic transaction reports per record retention schedule
End

Explanation of Transaction Security Levels

Level A	Under Level A security, state agencies may use any technological means for processing these sets of electronic transactions and providing assurance of authentication, nonrepudiation and integrity.
Level B	Level B electronic transactions must use, at a minimum, one of the following two security procedures for authentication: (a) a unique user-ID and an alphanumeric password consisting of at least eight characters, or (b) a smartcard or physical device with a unique proprietary password as an alternative. Documentation must describe the authentication process including information on the initial registration process and the means used to prove the identity of persons registering.
Level C	Under Level C security, state agencies must wait for OIT to approve the transaction. In addition, the transaction must use digital certificates based on public key infrastructure (PKI) ***OR*** combine the use of a unique user-ID and an alphanumeric password consisting of at least eight characters with a smartcard or physical device. State agencies seeking approval of the password/physical device alternative must provide a description of the authentication process including information on the initial registration process and the means used to prove the identity of persons registering. Pursuant to section 1306.21 of the Revised Code and Executive Order 2004-02T, which may be found at http://www.ohio.gov/itp, OIT may require that state agencies use a common multi-agency smartcard or physical device infrastructure.
Level D	For Level D security, state agencies must wait for OIT to approve the transaction. State agencies must use a digital certificate issued under a PKI approved by OIT in combination with a unique user-ID and password consisting of at least eight characters AND a smartcard or physical device or biometric. Like Level C security, OIT may require state agencies use a common multi-agency infrastructure. Any state agency using a biometric must establish security policies to provide a high degree of assurance of the integrity and, if applicable, confidentiality of the biometric information. Agencies subject to policies issued under ORC section 125.18 shall conform to any OIT policies and standards published at http://www.ohio.gov/itp for security, interoperability and need. While state agencies may use higher levels of security than required by the transaction risk assessment, for biometrics, a state agency seeking to implement the use of biometrics must provide a justification to OIT.
NOTES	**For any transaction used at Levels B, C or D or any Level A transaction involving confidential data or a monetary transfer, the transmission of user-IDs and passwords must be encrypted using secure sockets layer or equivalent encryption when transmitted over the Internet.** **Currently, no agency has filed a transaction report requiring a level greater than Level B. However, this is mainly due to the fact that the financial threshold is based on a "per transaction" basis, not on a "total transaction" basis.**