Office of State Controller, and the North Carolina Department of the Secretary of State, and North Carolina Department of Cultural Resources, Division of Archives and Records

Digital Signature Policy Guidelines

Version 1.1

March 2014

Contains corrected links to documents

Table of Contents

1 Introduction

1.1 Purpose of Guideline

This document serves as a policy guide for the use of electronic signatures. It provides information on the following:

- State and Federal legislation on the use of electronic records and e-signatures
- Definition of e-signatures
- Expectations and goals for instituting an e-signature system
- Potential challenges including security and privacy; cloud storage; and electronic records management
- Business and legal considerations

1.2 Scope

This document serves to provide guidance on e-signature initiatives pursuant to the laws of North Carolina. This document speaks more generally to the use of e-signatures and does not reference a specific product or current contract with a third-party vendor. These guidelines apply to the following government entities: Executive Branch agencies, non-state agencies such as the University of North Carolina system and member campuses, instructional components of the Department of Public Instruction and the North Carolina Community College system, as well as local and municipal governments.

2 Electronic Signature Background

2.1 Legislation

Federal and state legislation on electronic signatures spans more than a decade and has evolved as technology changed. In 1998, the North Carolina state legislature passed the Electronic Commerce Act to facilitate "electronic commerce with public agencies and regulate the application of electronic signatures when used in commerce with public agencies." [1] In 1999, the Uniform Law Commission proposed the Uniform Electronic Transactions Act (UETA), to give legal recognition to electronic signatures. The act states, "if a law requires a signature, an electronic signature satisfies the law provided it complies with the provisions of this Article." [2] In 2000, the North Carolina legislature, along with 46 other states, enacted UETA.

On June 30, 2000, the U.S. Congress passed the Electronic Signatures in Global and National Commerce Act (E-SIGN). E-SIGN states that a contract or signature "may not be denied legal effect, validity, or enforceability solely because it is in electronic form."[3] On the federal level, this act gives electronic signatures the same legal validity as handwritten signatures.

In more recent legislation, North Carolina Session Law 2011-145, House Bill 200 6A.18, effective October 1, 2011, gave the Office of State Controller the task of planning, developing,

[1] Electronic Commerce Act (1998-127, s. 1.)
[2] Uniform Electronic Transactions Act. (2000-152, s. 1.)
[3] ESIGN, Pub.L. 106-229, 14 Stat. 464, enacted June 30, 2000, 15 U.S.C. ch.96

and implementing "a coordinated enterprise electronic forms and digital signatures capabilities. In developing this capability, the State Controller shall determine the cost of converting forms to an electronic format, determine priorities for converting forms, and establish milestones for completing this conversion."[4] The law also states that all executive branch agencies that have already started any electronic forms or digital signature projects would be integrated into the State Controller's initiative.

The State Controller's office formed a workgroup to establish requirements for implementing a digital signature management system and investigate potential providers. Representatives from nine different agencies – DOJ, DOT, DOR, DPS, AOC, DHHS, Sec. of State, Cultural Resources, and Industrial Commission— participate in the Authentication Workgroup.

The workgroup set criteria for digital signatures software. It is necessary that a digital signature:

- Be secure.
- Provide auditable evidence that appropriate processes have been followed.
- Be easily used by individuals for ad hoc signing.
- Integrate with automated business processes.

Details on how digital signatures can meet the criteria above are listed in Section 2.1 *Intended Goals*.

2.2 Definitions

Application Programming Interface (API): The programming instructions that allow an application program or web tool (such as an e-signature system) communicate with the operating system or other control program that is attempting to access that application.

Authentication: Authentication is the process of verifying that a document or record is genuine or original. In the case of electronic documents, it is the process of confirming a user's identity.

Cloud Computing: The National Institute of Standards and Technology (NIST) defines cloud computing as a "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[5]

Digital Signatures: A complex string of electronic data that is embedded in an electronic document for the purposes of verifying document integrity and signer identity.[6]

Electronic Signatures: 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.[7]

Electronic record: A record created, generated, sent, communicated, received, or stored by electronic means.[8]

[4] N.C. Session Law 2011-145 House Bill 200
[5] Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing (Draft),* NIST, January 2011. http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf
[6] Uniform Real Property Electronic Recording Act. (2005-391, s. 1.)
[7] ESIGN, Pub.L. 106-229, 14 Stat. 464, enacted June 30, 2000, 15 U.S.C. ch.96
[8] Uniform Electronic Transactions Act. (2000-152, s. 1.)

Hash function: A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions are specified in FIPS 180-3 and are designed to satisfy the following properties:

1. (One-way) It is computationally infeasible to find any input that maps to any new pre-specified output, and
2. (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.[9]

Metadata: Metadata is structured information that describes, explains, and/or locates an electronic file. Metadata provides answers to questions like "what is it," "where did it come from," and "who created it?"[10]

Private key: A cryptographic key that is used with an asymmetric (public key) cryptographic algorithm. For digital signatures, the private key is uniquely associated with the owner and is not made public. The private key is used to compute a digital signature that may be verified using the corresponding public key.[11]

Public key: A cryptographic key that is used with an asymmetric (public key) cryptographic algorithm and is associated with a private key. The public key is associated with an owner and may be made public. In the case of digital signatures, the public key is used to verify a digital signature that was signed using the corresponding private key.[12]

Records Retention Schedule: A document that identifies and describes an organization's records, usually at the series level, and provides instructions for the disposition of records throughout their life cycle.[13]

Software as a Service (SaaS): Software applications are remotely owned or managed by the provider and are accessible to users through a client, typically the Internet. The user controls neither the underlying infrastructure nor applications. Examples of SaaS applications include web-based email, iCloud©, GoogleDocs™, Dropbox©, and Survey Monkey. ™[14]

2.3 Definition of an Electronic Signature[15]

UETA 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."[16]

The intent of UETA is to create a legal framework that allows agencies to seamlessly integrate electronic processes into transactions that previously had been done on paper. Therefore,

[9] "FIPS PUB 186-3 Digital Signature Standard (DSS)." National Institute of Standards and Technology, June 2009. <http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf>.
[10] "Metadata as a Public Record in North Carolina: Best Practices Guidelines for Its Retention and Disposition." North Carolina Department of Cultural Resources, Nov. 2010. Web. <http://www.records.ncdcr.gov/guides/Metadata_Guidelines_%2020101108.pdf>.
[11] "FIPS PUB 186-3 Digital Signature Standard (DSS)." National Institute of Standards and Technology.
[12] "FIPS PUB 186-3 Digital Signature Standard (DSS)." National Institute of Standards and Technology.
[13] "A Glossary of Archival and Records Terminology." Society of American Archivists
[14] "Best Practices for Cloud Computing Records Management Considerations." North Carolina Department of Cultural Resources. August 2012. Web. < http://www.records.ncdcr.gov/guides/cloud_computing_final_20120801.pdf>
[15] Modeled after: "Best Practice Guideline: Electronic Signatures and Records Act (ESRA) Guidelines." New York Office of Information Technology Services. 2007. Web. < http://www.its.ny.gov/policy/G04-001/G04-001.pdf>
[16] ESIGN, Pub.L. 106-229, 14 Stat. 464, enacted June 30, 2000, 15 U.S.C. ch.96

UETA's definition of electronic signature allows for a broad spectrum of technologies to be used, which gives the state flexibility when choosing an e-signature vendor. However, UETA does set some parameters on what constitutes an e-signature:

"[A]n electronic sound, symbol, or process"

An electronic signature can be a wide array of digital objects including a set of keyboard characters used for passwords to a more sophisticated encryption model. It is important to note that a process can serve as an electronic signature. A process is documented when the e-signature system creates a virtual historical record of the signer's actions as the signer attaches additional data to the document. Most e-signature systems will use a signing process in conjunction with the use of a digital object such as a PIN or password to authenticate the signer.

"[A]ttached to or logically associated with…"

This language means that an e-signature becomes part of the electronic record throughout that record's lifecycle, including storage after the transaction has been completed. It is similar to how an ink signature becomes part of a physical paper document and remains on the paper after it's been filed. Linking an e-signature to its electronic record can be done in multiple ways including embedding the signature into the document or maintaining the signature separately but "logically" in a database or index. The electronic signature needs to remain associated with the signed record for as long as the document has a legal effect and until the record can be disposed of based on its retention schedule. The signature is proof of the signer's intent and actions as described in the e-record.

"[E]xecuted or adopted by a person with intent to sign the record."

A signer should have the same intent in signing an electronic document that he or she would have in signing a paper document with pen. This means it is important for the signer to understand that an electronic document has the same legal weight as a paper document and that the signer intends to carry out whatever is stated in the document.

There are several ways to ensure that a signer understands the document he or she is about to sign:

- Allow the signer to review the entire document before applying an e-signature.
- Let the signer know that an e-signature is being applied.
- Provide a consumer disclosure that outlines the terms of conditions of using the e-signature signing system.
- Use electronic documents that are similar in style and format to the documents your agency uses in paper form.
- Place electronic tags indicating where signers need to provide additional information, add initials, or sign.

2.4 Electronic Signature versus Digital Signature

The terminology "electronic signature" and "digital signature" are often used interchangeably, but the two types of signatures are different. All digital signatures are a type of electronic signatures, but electronic signatures encompass a wide array of signer identification methods beyond just a digital signature. Some common e-signature methods include:

- ***Click through***: A signer clicks a button to affirm his or her agreement to the contents of a document.
- **Personal Identification Number (PIN) or password:** A signer will provide identifying information to the system, which may include their name and email address. Then the signer will either choose or be given a password or PIN number that will allow them to access the system. Security measures are built into these systems in case the signer forgets their password or PIN.
- **Digitized Signature:** A graphical image of a handwritten signature includes scanned images of ink-and-paper signatures or a signature created using a digital pen and tablet.
- ***Public Key Infrastructure (PKI) /Digital Signature:*** Additional information below.
- ***Biometrics:*** A signer's unique physical characteristics that are converted to digital form for interpretation by a computer. Voice patterns, fingerprints, and eye scans are all examples of biometrics.

A digital signature is one type of electronic signature. North Carolina Electronic Recording Standards define a digital signature as "a complex string of electronic data that is embedded in an electronic document for the purposes of verifying document integrity and signer identity."[17] A digital signature authenticates the identity of a user and certifies the secure transfer of electronically-signed documents through public-key cryptography. For more information on public-key cryptography see section 3.1 Security and Privacy. Levels of authentication for digital signatures include *click-to-sign* as well as *higher assurance needs*. Click-to-sign, the most common digital signature, uses ID and password for authentication. Once a document is digitally signed, the document and certificate of completion are locked and changes can no longer be made to the document. Higher assurance needs place higher proof-standards on the document such as voice signatures or biometric handwritten signatures.

3 Expectations for Electronic Signatures

3.1 Intended Goals

- **Security and Legal Compliance:** The e-forms and e-signature system provides a secure method of signing and transferring documents electronically. A document cannot be altered after the signer has completed the e-signature. Additionally, a history of any changes made to the document prior to the signature is kept with the document and cannot be changed or deleted. When digital signatures are used, hash values are attached to the document to verify the authenticity of a document during any transfer for added security.

- **Simplified workflow:** E-signatures eliminate resource-intensive processes that require agencies, citizens, and staff to manually sign documents**.** Features of the e-signature process include automation of simple forms**,** ability to track and review changes, vary the recipient roles, tag signatures; etc.

- **Integration into business processes:** The program must fit into pre-existing business practices, provide automated processes, retrieve documents, use standard APIs, generate reminders and expiration settings, and allow multiple people to view a document and track its progress.

[17] North Carolina Electronic Recording Standards. (2005-391, s. 1.)

- **Cost benefits:** There is a potential cost-savings from not having to print, file, and store paper copies. The State will save also on certified mail, postage, printing, ink, envelopes, and paper.

- **Integrate and utilize SaaS model:** The program must be flexible enough to incorporate the use of Software as a Service (SaaS) e-signature authentication model. This model allows users to automate, send, sign, and return documents inside one program that runs on a cloud platform. Additionally, since the platform is SaaS, the e-signature system can be used with any operating system.

3.2 Eligibility

The e-signature service offered by the Office of the Information Technology Services to other state agencies is a SaaS e-signature technology. Executive Branch agencies, the University of North Carolina system and member campuses, instructional components of the Department of Public Instruction and of the North Carolina Community College system as well as local and municipal governments are all eligible to participate. Interested groups can contact DocuSign directly to determine how to best implement this software into their daily business practices.

Contact information can be found at:
http://www.its.nc.gov/programs/eForms.aspx

4 Addressing Challenges

4.1 Security and Privacy

For digital signatures, public-key infrastructure (PKI) cryptography is used to ensure security and validity of transferred documents. A digital signature uses an algorithm to generate and verify itself. The Digital Signature Standard specifies three algorithms—Digital Signature Algorithm (DSA), RSA, and Elliptic Curve Digital Signature Algorithm (ECDSA) approved by the National Institute of Standards and Technology (NIST). Any digital signature software providers should use one of these approved algorithms.

To ensure the authenticity of a digital signature over time, the algorithm is used in two ways: for signature generation and signature verification. When a signature is created, a public and private key are attached to it. The signer is the owner of that unique key pair. To prevent fraudulent signatures, the private key remains known only to the certificate authority which also assures that the same key is not recreated by another digital signature. Additionally, the signed document generates an approved hash function prior to being sent to the verifier.

Once the electronic document and its digital signature are completed and sent; the private and public keys in addition to the hash function will be used to authenticate the document to the verifier. Several assurances take place. First, the algorithm will make sure the public key is a mathematical match to the one attached to the signatory, and that the signer has ownership of both the public and private key for the document. The software will then verify the hash function, the public key, and data message to validate the authenticity of the document and digital

signature. This verification will occur automatically and the system will inform the user of the validity of the document.

Other types of e-signatures will have varying degrees of security measures. It is important to become familiar with the security and privacy features of any e-signature system. Additionally, it is important to take extra precaution when sending documents with Social Security numbers and other personal identifying information. General Statute 132- 1.10 states that a state agency cannot "require an individual to transmit the individual's social security number over the Internet, unless the connection is secure or the social security number is encrypted." Documents sent through the electronic signature client will be encrypted; however, every agency should make sure transactions are being made on a secure network especially if there is personal information in the document. Most electronic signature vendors will provide features that can conceal values such as Social Security or credit card numbers from being viewed by other signers. The agency must take all precautions necessary to protect private information.

4.2 Cloud Storage

Most e-signature providers have capabilities for clients to manage and store documents in the provider's private cloud. NIST defines cloud computing as a "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Cloud computing may also be referred to as infrastructure as a service. Typically, service is available on-demand and customers pay for the amount of service they use.

North Carolina has specific laws that dictate the use of cloud computing. According to Session Law 2012-142, House Bill 950; "the wide distribution of information technology facilities across multiple locations causes infrastructure and operational inefficiencies."[18] The law provides for the creation of a private cloud, where all components are state-run and owned. This means that the infrastructure supporting the private cloud must also be located within North Carolina's borders.

By exemption with this service, agencies can choose to store their records with the digital signature vendor or download them onto local servers. Agencies should be aware of the risks of storing documents in a vendor cloud, including breach of security. For more information, consult the *Best Practices for Cloud Computing: Records Management Considerations* at http://www.ncdcr.gov/archives/ForGovernment/DigitalRecords/DigitalRecordsPoliciesandGuidelines.aspx#cloud

4.3 Electronic Document and Records Management

The use of e-signatures and forms will create more transactions that are solely documented and remain electronic records. It is important to remember that all laws applicable to traditional government records are also applicable to electronic records, including public records and retention laws. Therefore, it is essential that sound electronic records management practices are followed. Agencies choosing to use digital signatures should:

[18] N.C. Session Law 2011-145 House Bill 200

- **Choose a consistent and practical file-naming convention**. In the digital signature software client, you will be responsible for keeping both template forms and each completed form organized. There will be a higher volume of digital records to maintain since this process will transfer most paper forms to strictly electronic. To manage the extra volume, save completed forms in a manner that makes them easily recognizable and searchable. For more information, see the Best Practices for File-Naming at http://www.ncdcr.gov/archives/ForGovernment/DigitalRecords/DigitalRecordsPoliciesandGuidelines.aspx#filenaming. Or view instructional videos on file-naming convention at http://digitalpreservation.ncdcr.gov/tutorials.html.

- **Maintain the associated metadata.** Each electronic form uploaded or created in the digital signature software will have metadata that describes, explains, or locates the form. Metadata can be generated by the system, software, or the user. Examples of metadata include date, time stamp, file title, custom tags, and authors. The system will automatically generate some information such as the time stamp. The creator will be able to add descriptive information including, but not limited to, recipient instructions, transaction numbers, and additional identity check functions. Additionally, the system should create a summary report that includes a certificate of completion, record tracking, IP addresses, time stamps, and other important data that validates the document. This summary report is saved with the document in the digital signature client but can also be downloaded in a zip file with the document to be saved on the state server. To maintain the authenticity of the document it is imperative to save certain metadata fields including date, title or file name, name of the signers, and the time stamp. By saving the summary report with the document, all of this important metadata will be kept. For more information on retaining metadata as a public record, see the following best practices guide:
  http://www.ncdcr.gov/archives/ForGovernment/DigitalRecords/DigitalRecordsPoliciesandGuidelines.aspx#metadata

- **Follow all record retention schedules.** Electronic documents created in the transaction of public business are public records, and are subject to the Public Records Law and need to be retained according to a records retention and disposition schedule. As software and file formats change, it will be impossible to retain the digital signature intact. For records retention purposes, the signature does not need to be maintained; only the metadata documenting that the signature was verified when the transaction occurred. Examples of proving verification include the certificate of completion or summary report that is saved with the e-form. Records with long-term value should be removed from the digital signature client after completion and saved on a state server. When downloading these records, be sure to download the document as well as any envelope information containing the transaction metadata documenting the signature and authenticity. For records with short-term value, the digital client may allow the user to set automatic retention and disposition rules. Before using these automatic features, check with the client account manager to ensure the features will legally fulfill the agency's responsibilities of disposing of records on schedule. For more information on maintaining electronic records, see the online tutorial Managing Electronic Public Records: Recognizing Perils and Avoiding Pitfalls located at http://www.records.ncdcr.gov/tutorial_erecs_20081027/index.html. To find your records retention schedule, please visit (url to be filled in when new website is launched)

5 Business and Legal Considerations

Before opting into the e-signature system, assess your agency's business and legal requirements. Having a clear understanding of your agency's needs can help make the process of integrating the e-signature system more seamlessly into your day-to-day business transactions.

5.1 Legal Requirements and E-Signature Exceptions

UETA gives legal authority to e-signatures. Specifically, the law states that "a record or signature may not be denied legal effect or enforceability solely because it is in electronic form." Contracts also may not be denied legal effect if they are formed electronically. The act also states that as long as electronic records satisfy other applicable laws, then an electronic record and e-signature can be used in legal transactions.

Although UETA encompasses most transactions; there are some exceptions to its scope. UETA does not apply to a "law governing the creation and executing of wills, codicils, or testamentary trusts." According to NCGS §66-313, UETA does not apply to the following transactions:

- Any notice of cancellation or termination of utility services, including water, heat, and power
- Any notice of default, acceleration, repossession, foreclosure or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual.
- Any notice of the cancellation or termination of health insurance or benefits, excluding annuities.
- Any notice for the recall of a product, or material failure of a product that risks endangering health or safety.
- Any document required to accompany the transportation or handling of hazardous materials, pesticides, or other toxic, or dangerous materials.

If you have any questions about whether any of your electronic documents fall under these exceptions contact your agency's legal counsel.

5.2 E-Notarized Documents

The Uniform Electronic Transactions Act provides that if a document requires a signature to be notarized, the requirement is satisfied if the person authorized to perform the notarial act utilizes an electronic signature meeting the requirements of UETA and follows other applicable laws. The Electronic Notary Act in conjunction with the Electronic Notary Administrative Rules provide clear guidance for performing an electronic notary act, registering as an electronic notary, and selecting an approved electronic notarization solution. The notary's signature, all additional signatures, and applicable information must be "attached to or logically associated with the

signature or record."[19] For more information on E-Notaries, please visit http://www.secretary.state.nc.us/enotary/thepage.aspx

5.3 E-Discovery

Electronic Discovery (E-Discovery) is the legal process of gathering all relevant electronic information from the two parties involved in a lawsuit. Amendments to the North Carolina Rules of Civil Procedure, effective October 1, 2011, make electronically stored information (ESI) and "reasonably accessible" metadata discoverable, including those records saved in the digital signature client.[20] Records saved in the cloud must be accessible for legal purposes making it essential to follow agency record retention schedules. It is the responsibility of the agency to make these records available in the case of litigation; therefore, it is recommended to save records with long-term value to a state-owned server to protect against data destruction or from being accidently overwritten in a third-party client.

5.4 E-Signatures in Business Transactions

Not all signed documents are legally mandated, but rather serve as a record of a business transaction. According to the Electronic Commerce Act, e-signatures contained in a transaction "between a person and public agency, or between public agencies shall have the same force and effect as a manual signature."[21]

The Electronic Commerce Act stipulates that an e-signature used in a transaction must have the following attributes:

- It is unique to the person using it;
- It is capable of certification;
- It is under sole control of the person using it;
- It is linked to data in such a manner that if the data are changed, the electronic signature is invalidated; and
- It conforms to the rules adopted by the Secretary of State[22]

The State Controller's office and accompanying workgroup will ensure that any vendor chosen to provide e-signature services meet these qualifications.

6 Conclusion

The E-Signature initiative is intended to make state business practices more efficient. The process eliminates the need to print, file, and store paper copies of documents that can now be authenticated digitally and stored electronically either with the vendor or on state servers. Due to the potential high volume of documents being saved solely in electronic format, agencies will have to follow a solid electronic records management plan and consult the State Archives of North Carolina for guidance at www.records.ncdcr.gov.

[19] Uniform Electronic Transactions Act. (2000-152, s. 1.)
[20] Kara Millonzi, "Metadata, E-Discovery, and E-Public Records in North Carolina," September 15, 2011 http://sogweb.sog.unc.edu/blogs/localgovt/?p=5432.
[21] Electronic Commerce Act (1998-127, s. 1.)
[22] Ibid.

7 Additional Information

Uniform Electronic Transactions Act (UETA):
http://www.ncleg.net/EnactedLegislation/Statutes/HTML/ByArticle/Chapter_66/Article_40.html

Electronic Commerce Act:
http://www.ncleg.net/EnactedLegislation/Statutes/HTML/ByChapter/Chapter_66.html

Office of Information Technology Services eForms and Digital Signatures:
http://www.its.nc.gov/programs/eForms.aspx

Department of the Secretary of the State: Laws Governing Electronic Commerce
http://www.secretary.state.nc.us/enotary/enotarylaws.aspx