



**North Carolina
Enterprise Electronic Forms and Digital
Signatures**

**Quarterly Report
October 2011**

**North Carolina
Office of the State Controller**

**David McCoy, State Controller
October 1, 2011**

Table of Contents

I. Background:	4
II. Enterprise Electronic Forms and Digital Signatures	5
A. Objective.....	5
B. Approach	7
C. Tasks Initiated or Completed To Date	8
D. Timeline.....	8
E. Challenges.....	9
Appendix A: Session Law 2011-0145, House Bill 200	10
Appendix B: Prior Studies	11
Appendix C: References	13
Appendix D: Key Definitions	14

I. Background:

As we approached the turn of the century, North Carolina state government entered into the world of e-government and e-commerce with the adoption of several bills by the General Assembly.

e-Commerce

In 1999, SB222 directed and authorized the Office of State Controller to begin the development of a statewide enterprise infrastructure to accommodate electronic payments. This electronic payment program now has three components:

- Electronic Funds Transfer (EFT).
- Merchant cards (debit and credit cards): using an enterprise approach, OSC arranged for a “Master Services Agreement” (MSA) with external service providers under which agencies could participate.
- Inter/Intra governmental transactions involving transfer of funds between agencies, each having an account with the State Treasurer.

In addition to the electronic payment program, two gateway services were established and are now offered for accepting payments through the web:

- Common Payment Service (CPS) which is offered by the Office of Information Technology Services and
- PayPoint Gateway offered by First Data Government Services (FDGS) through SunTrust Merchant Services (STMS) and provides a web “consumer interface” component.

e-Government

Many agencies have made progress in automating some of their internal and external processes for gathering data. Some examples include: duplicate driver’s license, tax filing, pesticide license renewal, vehicle registration renewal, and a youth work permit application.

The Office of Information Technology Services has developed:

- Enterprise service for Electronic Document Management (EDM). This service allows an agency to develop workflows for documents, to restrict access to information to appropriate groups of users, and to maintain controls on versions of documents in a repository. Some agencies are using content management tools independent of or outside of the ITS Enterprise Service.
- North Carolina Identity Management (NCID) for personal authentication, which uses the pin-password form of digital identity; however it has been designed to handle stronger methods of authentication.

The Office of the Secretary of State has established two significant programs built around the concept of electronic signatures.

- The first is the creation of the E-Notary program. It follows the concepts of the original notary public – a person with special training verifies that a signature was executed in his or her presence and by affixing a seal, certifies that the signature is valid. Now, the E-Notary can use an electronic signature to certify the signature’s validity.

- The second program at the Office of the Secretary of State involves the electronic filing of real estate records. The creation of this program was authorized by the General Assembly in the Uniform Real Property Electronic Recordation Act. It allows real property documents to be electronically recorded in registers of deeds offices.

The Enterprise Project Management Office (EPMO), under the Office of Information Technology Services, currently has several automation projects in the State’s portfolio of projects: ESC Document Management Project, DPI Licensure Automation System, OSP E-Recruit Project, and the Health Care Facility Business Process Automation systems. The latter will use NCID for authentication.

Despite these successes, the State has seen slow progress in the area of automation and authentication adoption. This is partially due to the large volume of forms and transactions in state government and the failure to provide services with flexible options and competitive price points.

Unlike the past, our current government agencies and their staff have technology expectations as they use social media, shop online and use kiosks everywhere – the movie theatre, ATM, airports and etc. The question that must be resolved is how can government keep up with the technological expectations of citizens, agencies, and staff?

To address this question the State must have a customer focus that is responsive, that embraces a vision for automation and authentication and allows “self-service” while moving the State to a position to better manage the “new normal” of reduced budgets and staffing levels.

II. Enterprise Electronic Forms and Digital Signatures

In the past, on three prior occasions, the legislature requested that an enterprise e-forms and e-signature capability be developed. (See Appendix B for a description of these efforts.) Session Law 2011-0145, House Bill 200, directed the State Controller to take the necessary measures to enable a coordinated enterprise electronic forms and digital signatures capability.

While some successes have been achieved—the State’s HR/Payroll system is an enterprise-wide timekeeping and payment system and e-Recruit will soon automate the State’s recruitment and hiring practices—most successful automation activities have had a narrow purpose. OSC’s intent is to provide solutions that are nimble and can be replicated, and can help agencies solve a wide variety of automation problems.

Along with the limitations of programs being too narrowly focused, OSC is also aware of the risks associated with casting the net too wide. The current focus is on automating business processes rather than on the broad universe of e-government.

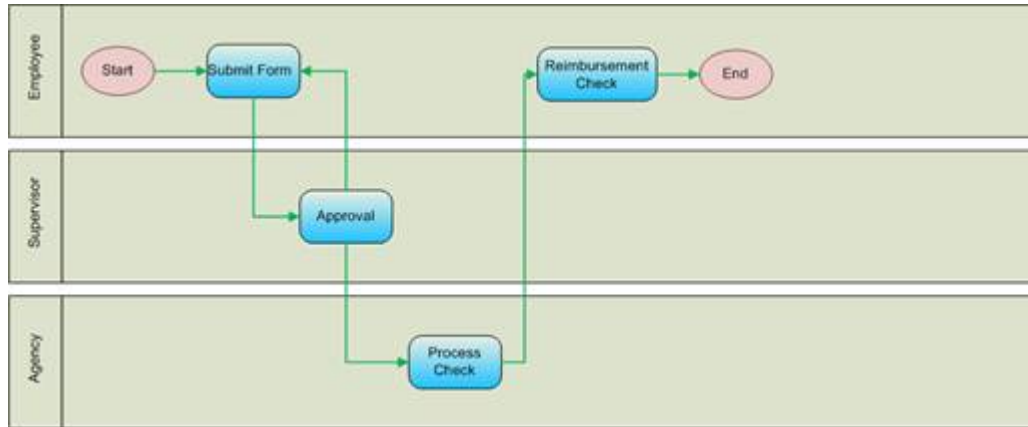
A. Objective

OSC shall work collaboratively with appropriate State agencies and research best-practice methods to obtaining automation and authentication capabilities, including cloud-hosted, on-premises rental, managed via outsourcers, and open-source software.

Rather than simply making forms electronic, OSC proposes reframing of the “e-forms” initiative to focus on eliminating paper forms with a concurrent introduction of workflow automation that will reduce processing times, eliminate duplicate data entry, improve data integrity, and provide for on-line service options.

The levels of automation can be broken down into three main areas:

- 1) Front-end collection of data;
- 2) Workflow and approval processes; and
- 3) Data capture and storage.



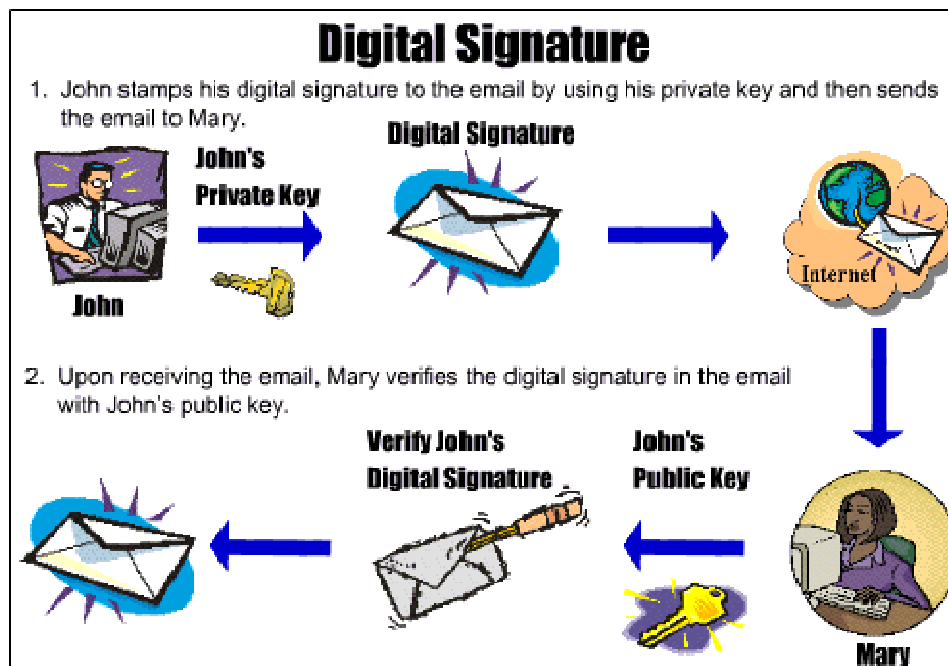
OSC shall assist and collaborate with agencies to determine the levels of automation that provide maximum benefits for the identified funding and set priorities accordingly. The benefits will vary depending on the agency business processes.

Regarding digital signatures, OSC recognizes that certain agencies will have unique requirements. Therefore, given the need for agency-specific levels of authentication, OSC will work with agencies to ensure that they have a variety of cost effective solutions.

A digital signature ensures a higher level of authentication than a hand-written signature – giving the recipient reason to believe that the message was created by a particular and known sender and that it was not altered in transit. OSC will work to provide offerings that are secure, provide auditable evidence that appropriate processes have been followed, can be easily used by individuals for ad-hoc signing, and can be integrated with automated business processes.

The levels of authentication can be broken down into two main areas:

- (1) “Click-to-sign” – the most common type of electronic signature – uses ID and password as authentication. Contextual information, such as date, time, IP address of the signing device, and its geo-location may be stored within the document or noted in an audit record. This contextual information and authentication and the integrity properties are usable for evidence if needed.
- (2) “Higher assurance needs” where additional proof (additional factors) of authentication is needed (e.g., NCID or, for even greater authentication, digital signatures). This may require partnering with a third-party for additional voice signature, biometric hand-written signatures or other verification methods.



OSC will work with agencies to determine:

- The level of authentication needed.
- The volumes of transactions required by level.
- The best method of delivering offerings to satisfy the varied needs of the agencies.

OSC also will work with agencies to weigh the level of risk against security and ease of use when evaluating authentication systems.

B. Approach

Recognizing the separate statutory authority under which agencies operate, statewide enterprise programs must be structured to accommodate the variety of operational needs unique to each government agency and to each entity within that agency. Therefore, OSC will leverage the same approach used for the e-Commerce Program by:

- Gathering information from other states to determine areas of focus, tools used, efficiencies and improvements realized.
- Meeting with agencies to gather their detailed business requirements, timelines, and metrics for measuring success.
- Conducting industry research on tools and technologies that are available and the most appropriate methods of delivery: software as a service (SaaS), or on-premise software solutions, or others.
- Reviewing the consolidated findings and making a build-versus-buy decision – recognizing that it may require multiple solutions to fit the various business needs. In State government's complex environment, a one-size-fits-all solution may add unnecessary complexity to simple operations and slow operations that are more complex.
- Developing cross-agency functional teams to review and evaluate deliverables throughout the project.

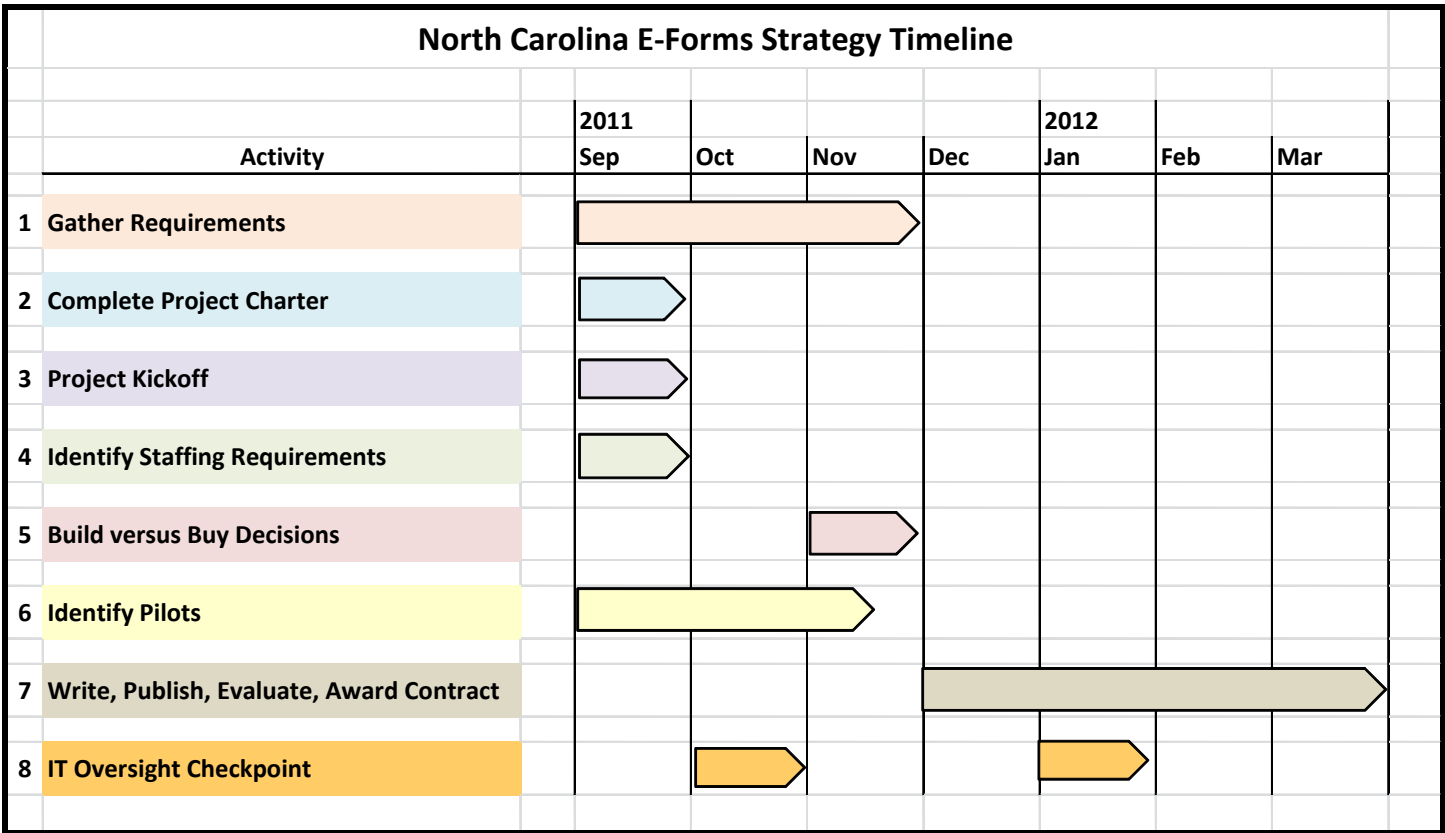
- Establishing an ongoing process for identifying potential candidates for automation and authentication.
- Developing an on-boarding process for identified agencies to take advantage of the automation and authentication tools.

C. Tasks Initiated or Completed To Date

- Projects assigned to Director of e-Commerce (OSC)—completed.
- Resources assigned to the project from the State Chief Information Officer (per legislation)—completed.
- Call with third-party information technology research and advisory firm (Gartner) on authentication—September 27th
- Requirements documentation—initiated.
- Project initiation meetings include the following:

Agency	Date	Status
ESC	Aug 15 th	Complete
Community Colleges System Office	Sept 7 th	Complete
Dept of Justice	Sept 15 th	Complete
Dept of Agriculture	Sept 16 th	Complete
DHHS – MMIS	Sept 27 th	Complete
DHHS - HIT	Sept 30 th	Complete
Dept of Correction	Sept 30 th	Complete
Dept of Labor	Oct 3 rd	Scheduled
Sec. of State	Oct 4 th	Scheduled
DENR	Oct 17 th	Scheduled
Dept of Transportation	TBD	Contacted
Cultural Resources	TBD	TBD
DHHS – NCFAS	TBD	TBD
Dept of Treasury	TBD	TBD

D. Timeline



E. Challenges

OSC has identified several challenges that could inhibit the successful implementation of the Electronic Forms and Digital Signatures project. They include:

- Project scope. The project must be scaled and right-sized into manageable and deliverable components.
- Agency participation. Collaboration, support, and agency commitment are essential to achieve established goals for this initiative.
- Cost-effective solution. There is not a single solution that will meet every agency’s needs. Therefore, efforts must focus on providing maximum and successful results, efficiency and cost savings for each agency.

Appendix A: Session Law 2011-0145, House Bill 200

Session Law 2011-0145 asked the State Controller to provide enterprise capability for e-forms and digital signatures. The law requires that costs, priorities and milestones be determined. Agency requirements must be incorporated into the planning process.

SECTION 6A.18.(a)

Under the direction of the State Controller, the State shall plan, develop, and implement a coordinated enterprise electronic forms and digital signatures capability. 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. The State Controller shall integrate executive branch agencies already in the process of developing electronic forms and digital signatures projects. Before beginning this effort, the State Controller shall determine specific agency requirements and incorporate their requirements into its planning efforts.

SECTION 6A.18.(b) Beginning October 1, 2011, the State Controller shall present quarterly reports on the status of the project to the Joint Legislative Oversight Committee on Information Technology.

Appendix B: Prior Studies

OSCIO, Electronic Document Management and Digital Signatures for North Carolina State Government, April 2009

This report describes a pilot program for electronic document management with digital signatures. The pilot had two parts:

- An Alcohol Beverage Control Commission form was created in PDF format that could be filled, digitally signed, and submitted electronically.
- BEACON, the state's payroll and human resources system, was created to modernize and standardize a key business process.

A recent breakthrough in digital signatures is described in this report when the Secretary of State's office created an e-notary program and allowed for the filing of real estate records electronically.

Policy and statutory issues include information overload, the lack of a complete inventory of state forms (which number in the tens of thousands), the lack of constituent services for citizens, and the lack of a central group mandating e-services and e-government.

The report recommends that:

- OSBM should create an inventory of paper and electronic forms.
- OSBM, ITS and DCR should develop a plan for e-forms and digital signatures.
- A steering committee should advise on policy issues regarding records retention, training and operational governance for e-forms.

OSBM, Use of Electronic Forms and Digital Signatures Report, March 2010

This report provides recommendations to increase the use of electronic forms and digital signatures throughout state government. It offers definitions of key terms, and a limited inventory of forms in state government (those deemed by agencies to have a high potential for automation). The report discusses challenges to electronic automation; the three overriding issues that limit progress are:

- (1) Agency and statewide organizational barriers.
- (2) Lack of understanding or urgency among agency managers.
- (3) Absence of central technological solutions, policy and assistance.

An e-form maturity model is provided, as well as a methodology for assessing the need for automating a given business process.

The OSBM report has five recommendations:

- (1) More centralization for state information policy and infrastructure.
- (2) Build technical expertise at ITS.
- (3) Map an as-is state business process and information architecture.
- (4) Create an incentive to automate forms.
- (5) Dedicate resources.

OSCIO, Electronic Forms (e-Forms) Initiative, October 2010

This report describes a maturity level for e-forms, from paper based, to consolidation, to a fully managed and optimized e-forms environment. The highest maturity level provides the most value (but at a high cost) with the least complexity. Levels of authentication are briefly described, with the highest level being digital signatures.

The 2010 OSCIO report has five recommendations:

- (1) Use the OSBM inventory to categorize and prioritize the opportunities for e-forms.
- (2) Use the e-form funds to create an Ethics Commission form and launch the E-Recruit project as case studies.
- (3) Leverage the State Enterprise Portal project vendor, which should have a set of built-in applications and e-form toolsets (The State does not currently have legislative authority to enter into that contract.)
- (4) Hire a project coordinator.
- (5) Establish an e-forms Center of Excellence.

Appendix C: References

North American and European Electronic Signature Suite and Service Market, January 2010, Gartner Research – ID Number: G00173599.

In the North American E-Signature Market, SaaS Offerings Are Increasingly in Demand, August, 2011, Gartner Research – ID Number: G00215378.

Magic Quadrant for Enterprise Content Management, November 2010, Gartner Research – RAS Core Research Note G00206900.

Appendix D: Key Definitions

Application: An application is any automated solution that facilitates business processes online. The business process may be one that is specific to one agency or business unit, or it may be a generalized process shared by many agencies (such as applicant tracking, grant administration or budgeting). Applications are often web-based.

Authenticate: The process of determining whether someone is, in fact, who the person declares to be. This is commonly done by the use of logon passwords. Other means of authentication, especially with regard to e-forms, include electronic signatures or notarization.

Business Process: A collection of interrelated activities, initiated in response to a triggering event, which achieves a specific, discrete result for the customer and other stakeholders of the process. The result of the business process must be discrete, countable, and fundamentally necessary to the operation of the organization. An example of a business process could be: “Admit (or Reject) License Applicant.”

Business Process Reengineering (BPR): A management practice that aims to improve the efficiency of the business process.

Digital Signature (Strong Authentication): An electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

e-Form: An e-form is digital representation of a paper form where the end-user fills in required information into fields, and then submits the form to the appropriate party electronically. E-forms systems typically include features such as validation (to ensure that required fields are completed, or that data is entered in a required format), in-line help (to explain the purpose of sections or fields in the form), and may include digital signatures (to allow the end-user to legally ‘sign’ the submitted form without using paper). Advanced e-form solutions are “applications” (see above).

Non-Repudiation: Services that 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.

Simple Authentication: If a digital signature (see definition above) is not required, a pin-password pair can constitute a valid, though less stringent form of authentication. Pin-password pairs are a type of personal credential or identity, much like a passport or driver’s license. For example, because a State employee has access to the State’s email system through pin and password, emails coming from that employee are assumed to be authentic.