Implementation of the ‘Digital Signatures’ in the State Government agencies of the Commonwealth of Virginia

Pilot Implementation

Executive Summary

07/15/2008
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Need and Background</td>
<td>3</td>
</tr>
<tr>
<td>Project Approach</td>
<td>4</td>
</tr>
<tr>
<td>Solution Description</td>
<td>5</td>
</tr>
<tr>
<td>Implementation Plan Key Steps</td>
<td>6</td>
</tr>
</tbody>
</table>
Introduction

The purpose of this document is to provide the need and background, summary of analysis, project approach to conduct a pilot for implementing PKI (Public Key Infrastructure) based ‘digital signatures’ in the executive branch agencies of the COVA (Commonwealth of Virginia).

Need and Background

DMME (Department of Mines and Minerals and Energy) expressed a business need for acquiring digital signature capability that will allow companies to submit digitally signed copies of maps and other technical documents to the agency in order to reduce the costs attributed to producing and handling bulky paper documents and improve application processing times. A similar need was expressed by VDOT (Virginia Department of Transport) for allowing their staff engineers and consultants to digitally sign the maps and engineering drawings.

In addition to VDOT and DMME there are many other state agencies like DGIF (Department of Game and Inland Fisheries), VDSS (Virginia Department of Social Services), various licensing boards and Secretary of the Commonwealth (e-notary) that have a potential use for this capability. The acceptability of digitally signed documents has increased significantly over the past few years and there are legislations and directives both at State and Federal Level that permit their use.

A digital signature solution would benefit the Commonwealth in a number of ways. First, by enhancing and expanding digital government, it would support the goal of “Best Managed State” This system would increase overall agency efficiency and citizen and industry’s perceptions of government performance. It would support Virginia’s goal of improving the climate for businesses operating in the Commonwealth.
Digital Signature Initiative

Project Approach

Our analysis of the requirements has shown that the transactions that can benefit from a digital signature can be categorized into 3 types:

Transaction 1.
Business to Government:

Business representative signs /certifies and submits documents to state agencies / departments.

Transaction 2.
Government to Government & Government to Business:

2.1 State employees sign and certify documents
2.2 Data exchange
2.3 Authentication for web services
2.4 Signing inter/ intra agency forms
2.5 Expense reports, Emails etc.
2.6 State employees sign and submit documents to businesses and vendors.

Transaction 3.
Individual to Government

On line forms and applications: where Individuals need to sign and submit the forms.

3.1. Category 1: Low confidence in the Identity of the person signing the document.
3.2. Category 2: High confidence in the Identity of the person signing the document.

As each transaction has its own unique requirements and constraints it makes it difficult to have a single approach for all transaction types. For the same reason it is best to implement the solutions in a phased manner.

Phase 1 of the project will focus on Transaction type 1 and Transaction type 2.1. A pilot will be conducted with VDOT and DMME and the results will be used to determine the best approach going forward.
Scope of the Pilot

The intent of the pilot is to focus on subset of transactions under Transaction type 1 and 2.1. The following scenarios will be addressed in the Pilot:

1. Situations that require business to submit documents that require a wet signature and possibly a professional seal with wet signatures for legal or statutory purpose. Documents type includes Engineering Drawings, Maps, etc. and the Formats included will be .pdf, MS document or Tiff.

2. Situations that require state employees to certify documents with wet signature and a professional seal for legal or statutory purpose. Documents type includes Engineering Drawings, Maps, etc. and the Formats included will be .pdf, MS document or Tiff.

Also it should be noted that: Vendors doing business with DMME and VDOT are engaged in business activities with other state agencies also, and those agencies may choose not accept the digital signatures till they have modified their processes.

Description of solution for the Pilot

A digital signature solution has two components:

1. **A Public Key Infrastructure (PKI) based Digital certificate:**
   Managed by a CA (certificate authority) that performs following tasks:
   a. Identity verification of the applicant and issuing of certificates
   b. Generating the physical certificate
   c. Managing the certificate life cycle

2. **Signature interface** – A Web service, client based or a combination of two. A solution that will allow a person to apply signatures to the documents.

Digital Certificate for the pilot

The pilot will be conducted using Identrust [http://identrust.com/](http://identrust.com/) as the CA. Identrust is a certificate provider and operates under the ACES (Access Certificates for Electronic Services) program.

ACES program provides digital certificates and Public Key Infrastructure (PKI) services to enable electronic government applications that require logical access control, digital signature and/or electronic authentication.
Digital Signature Initiative

GSA serves as a Policy Authority and is responsible for organizing and administering the ACES Policy and the ACES contract.

Link for ACES: http://www.gsa.gov/Portal/gsa/ep/channelView.do?pageTypeId=8199&channelPage=%252Fep%252Fchannel%252FgsaOverview.jsp&channelId=-13479

Link for Identrust Policies: http://identrust.com/certificates/aces_policies.html

Signature Interface for Pilot

There are many options for the signature interface. For this pilot we will be using ADOBE standard and other third party utilities.

Implementation Plan Key Steps

- Proposal approved by Chief Application Officer (CAO), Attorney General (AG), Pilot Agencies, Identity and Access Management Committee.
- Memorandum of Agreement (MOA) signed between VEAP (on behalf of COVA) and Identrust.
- Identrust creates Custom Web Pages for VDOT and DMME that will allow business and employees to apply for and procure certificates.

DMME:
- DMME will inform their customers and provide instructions on how to access and use.
- Business will pay for their certificates.
- Business will procure and pay for a signing interface of choice. DMME will provide recommendations for an interface based on previous research.

VDOT
- For their consultants:
  o VDOT will inform their customers and provide instructions on how to access and use.
  o Business will pay for their certificates.
  o Business will procure and pay for a signing interface of choice. VDOT will provide recommendations for an interface based on previous research.
Digital Signature Initiative

- For their employees:
  o VDOT will educate their employees and provide instructions on use and access.
  o VDOT will acquire and pay for their certificate using the GSA schedule.
  o VDOT will procure and pay for a signing interface of choice.

Key Milestones

<table>
<thead>
<tr>
<th>#</th>
<th>Mile Stone Description</th>
<th>Proposed Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Proposal distributed to CAO, AG, Pilot Agencies, Identity and Access Management Committee.</td>
<td>06/20/2008</td>
</tr>
<tr>
<td>2.</td>
<td>MOA (Between Identrust and VEAP) submitted to AG for review</td>
<td>06/20/2008</td>
</tr>
<tr>
<td>3.</td>
<td>Preliminary approval received from key stakeholders</td>
<td>07/10/2008</td>
</tr>
<tr>
<td>4.</td>
<td>VDOT initiates procurement process for signing Interface</td>
<td>07/15/2008</td>
</tr>
<tr>
<td>6.</td>
<td>MOA (Between Identrust and VEAP) approved by AG</td>
<td>07/25/2008</td>
</tr>
<tr>
<td>7.</td>
<td>MOA signed between VEAP and Identrust.</td>
<td>07/28/2008</td>
</tr>
<tr>
<td>8.</td>
<td>Identrust initiates creation of custom web pages for VA that will allow business and employees to apply and procure certificates.</td>
<td>07/25/2008</td>
</tr>
<tr>
<td>9.</td>
<td><strong>Digital signatures are available for use</strong></td>
<td>07/27/2008</td>
</tr>
<tr>
<td>10.</td>
<td>DMME begins training and implementation</td>
<td>07/27/2008</td>
</tr>
<tr>
<td>11.</td>
<td>VDOT completes procurement process for signing Interface</td>
<td>08/15/2008</td>
</tr>
<tr>
<td>12.</td>
<td>VDOT begins training and implementation</td>
<td>08/15/2008</td>
</tr>
</tbody>
</table>