

2009 NASCIO Recognition Award Nomination



Category: Information Security and Privacy

Title of Nomination: Enterprise Certificate Services

State: Maine

B. EXECUTIVE SUMMARY

In seeking to answer these questions and meet these security needs, the State of Maine determined the best way to ensure one identity for the State and one solution for security was to implement an enterprise solution using certificates to provide security services.

Business Need: With the impending need for the State of Maine Office of Information Technology (OIT) to replace an existing silo security system that provided security using certificates, a proactive approach was undertaken in 2006 to look at enterprise needs. The first step was the creation of a business case stating the need of establishing a standard enterprise approach to provide identity and security services. With the approval of the business case a stakeholder group began meeting to discuss the needs and a possible solution. The stakeholder group included representatives from all branches of government and the constitutional offices. This was the first time an enterprise initiative had crossed all branches of government and included all of the constitutional offices.

Business Solution: The consensus was to support the creation of an enterprise architectural solution that would be governed by representatives from the various branches and constitutional offices. This architectural solution would be the creation of a Certificate Authority (CA) to be built, managed and governed by the State of Maine.

Project Begins: The 'Certificates - Enterprise Resource for Technology Security' (CERTS) Project was launched. The OIT Project Management Office (PMO) assigned a full time project manager. OIT also assigned an Enterprise Systems Architect as a technical project manager and assigned ten OIT resources to the project team. With the recent centralization of the OIT, this was the first project to incorporate the enterprise approach of working across divisions and to have a team comprised of members from various divisions within OIT.

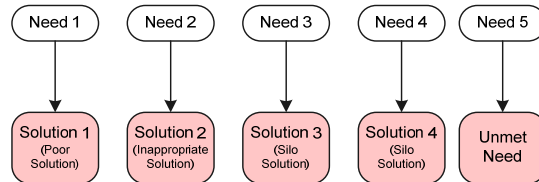
Because of a time-driven schedule imposed by the pending expiration of an existing system and because of the limited knowledge of this expertise, the decision was made to contract an outside technical expert to assist the OIT team in implementing the solution. The State of Maine contracted one of the leading experts in the technology of certificate services to assist with the design and implementation.

Solution Implemented: The solution was successfully implemented in November of 2007 along with a signing ceremony when the Secretary of State and Chief Information Officer signed the Certificate Services Policies and Practices document. The end result is an enterprise infrastructure providing authentication and secure information exchange with the use of certificates. From this enterprise architectural foundation the state has the facility to launch and provide detail security services to all branches of government and to all users of state services.

C. DESCRIPTION

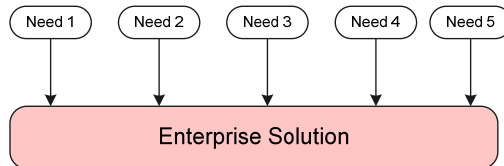
Business Problem:

- The OIT application providing security services using certificates needs replacement.
- State of Maine agencies are creating 1:1 solutions to meet security needs. Some of the solutions are acceptable. Some of the solutions are inadequate. Some of the solutions are inappropriate. Some of the needs are not being met.
- Users need separate security for each application accessed.



Business Opportunity:

- The need to replace the OIT existing application is an opportunity to build a solution that not only meets the immediate need for OIT but that will meet the security needs of agencies across state government.
- A standard approach to provide security services with the use of certificates will allow one certificate service to be used for all state computers, users, and services and will eliminate the need for multiple certificates to access various state computers and services.
- An enterprise identity management solution will prove identity one time, make it portable, and will establish a way to manage it.
- An enterprise solution will provide a ready-made solution as future security needs arise.

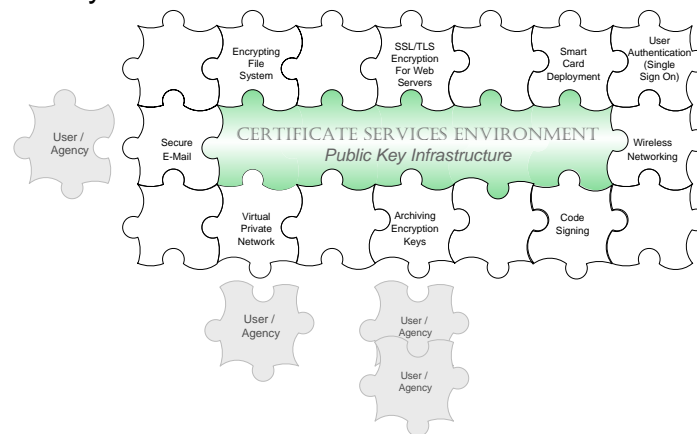


Business Solution:

- Stakeholders were presented with the question: “Should the State of Maine move forward with an enterprise solution or should the State of Maine build a solution that meets the Status Quo and replaces only the existing application that needs to be replaced?” A list was made of the Benefits and Risks of staying with the Status Quo and a list of Benefits and Risks of moving forward with an enterprise solution. After assessing the list of benefits and risks of each option, the stakeholder consensus was to move forward with an enterprise solution.
- The stakeholders then were presented with six options to meet this business need:
 - 1) Create a solution in-house, 2) use a combination of in-house resources with outside technical assistance, 3) outsource a solution that would be co-developed and co-managed, 4) outsource the solution and have it remotely hosted, 5) create an operational expedient solution that meets the immediate need and does not address an enterprise solution and is not a managed process, and 6) use certificate services without creating a Certificate Authority (purchase a-la-carte certificates). Information was presented to the stakeholders on each of the solutions including cost estimates

for each. Based on the budgetary and time constraints and the limited in-house knowledge of this technology, the recommended solution was a combination of in-house managed certificate services with outside expert technical assistance.

- This project overcame a great barrier in that this was the first initiative in the State of Maine that included all of the branches of government and each of the constitutional offices. This project is unique not only within the State of Maine, but it is unique in that few states have undertaken the initiative to build, own, and maintain their own Certificate Authority.
- The project included creating a Certification Policies and Practices Statement and the creation of a Certification Policy Management structure to govern the Certificate Authority (CA) policies and change management process.
- Using the analogy of building a house vs. building a commercial building, OIT decided to build an architectural foundation that has the capability to support many units rather than build the architecture to support a one-unit building. The infrastructure is built to meet Federal Certification specifications.
- The 'foundation' is a Public Key Infrastructure that provides the facility to support detail services and to provide the detail services to all users across all branches of State government and to all users of state services.
- The solution addresses building the foundation, the certificate services environment (the Public Key Infrastructure). The project also includes the launching of one service from this architecture: Wireless Networking service. The foundation provides the facility for future services to be provided, thus providing leverage for one solution to meet future security needs.



- The solution involved contracting an outside technical expert to assist the State of Maine OIT resources in implementing the solution. Other than the one contracted consultant, the project was fully managed and staffed with OIT resources. A full-time project manager from OIT's Project Management Office (PMO) was assigned to the project to manage the project from inception to implementation.
- The end result is an enterprise infrastructure providing authentication and secure information exchange with the use of certificates. A certificate is a digital representation (document) of electronic credentials along with a private and public key issued by a third party certificate authority. The architecture includes a Hardware Security Module, a Root CA and a Policy Issuing CA.

Project Management:

- The State of Maine OIT PMO follows the TenStep project management methodology. The project, scope, and deliverables were clearly defined in a project charter. A Quality Management Plan was followed to assure the quality of each of the deliverables.
- The State of Maine is the owner of the technology and is responsible for the continuing oversight and governance of the product.
- The total cost of the project was \$366,000, including \$60,000 materials, \$248,000 in-house resources, and \$58,000 for contracted expert technical assistance. The total effort was over 3000 hours of state resources. The initial estimate at the beginning of the project was \$310,000 - 370,000. The contractor's recommended design increased the estimate above the initial range. At a two-month checkpoint a decision was made to reduce the scope to keep the project expenses within the initial approved range. This was done by simplifying the architecture while at the same time ensuring that it would still meet the business need and maintain the structural integrity of the application.
- The project was implemented in production on November 28, 2007. It has been in production for more than eighteen months.
- The project has accomplished its objective by creating an enterprise architecture that has capability of providing security services to all branches of government and to all users of state services.

D. SIGNIFICANCE OF THE PROJECT

The solution improves the operation of government in the following ways:

- The implemented certificate service protects the confidentiality of information, provides security and encryption, and reduces the risk of security breaches.
- The solution is scalable. It is built to meet immediate needs and to accommodate future needs of state agencies and citizens.
- The solution is in alignment with Homeland Security Presidential Directive HSPD 12.
- The solution is in line with the Governor's vision of doing business once and not duplicating processes.
- The solution is in line with the recent centralization of OIT and demonstrates that the organization is functioning as an enterprise.
- The solution allows the State of Maine to have one identity presented to the public and will provide confidence and thwart spoofing of the State of Maine identity.
- The solution lays the ground work for interoperability of identity and encryption between state, federal, and business partners. The immediate beneficiaries include state agencies and users of state services and in the future will include federal and business partners and the public.
- This project incorporated formal project management and demonstrated the benefits of project management. Management previously perceived project management as an unnecessary overhead, but as a result of this project has seen first hand the value of formal project management and is eager to adopt the process for future projects.

- This project is significant in that few states have undertaken the initiative to build, own, and maintain their own Certificate Authority.
- This project is the first initiative in the State of Maine that crosses all of the branches of government and each of the constitutional offices.
- The creation of the Certification Policy Management structure that governs the Certificate Authority fosters cooperation and interaction across all branches of government and the constitutional offices.
- The project was completed on time, within budget, and successfully met the defined scope of the project. The scope of the project was clearly defined to 1) build a foundational architecture for a Certificate Authority to support internal services, Federal Certification, and external services (services to public users of state services); 2) establish Certificate Authority Management policies and practices, and 3) provide wireless services for internal certificate services.

E. BENEFITS OF THE PROJECT

\$230,648 Short Term ROI - Realized Benefits and Payback as of May 26, 2009:

- \$88,308 Configuration Savings: The technology that was in place prior to the certificate services implementation utilized Protected Extensible Access Protocol (PEAP) via RADIUS tied into Active Directory (AD) which required a 30 minute one-time laptop configuration for each use. The new technology eliminates wireless card configuration. As of May 1, 2009 the State of Maine has 2383 Wireless users and 2676 laptops configured for wireless utilizing the new services.
 - ⇒ Eliminated the wireless card configuration on 2676 laptops which represents an \$88,308 configuration savings (\$66 /hr staff time X 0.5 /hr X 2676).
- \$142,340 Avoided Annual Costs: By using our own internal Certificate Authority to generate the Computer and User Certificates we have:
 - ⇒ Avoided a \$76,420 annual computer certificate cost (\$20 /yr X 1145 year 1 and \$20 /yr X 2676 year 2)
 - ⇒ Avoided a \$62,420 annual user certificate cost (\$20 /yr X 738 year 1 and \$20 /yr X 2383 year 2)
 - ⇒ Avoided a \$3,500 annual RADIUS server and Certificate Authority (CA) Servers (Root, Polity & Issuing) certificate cost (\$350 /yr X 5 servers X 2 years)
- Resolved previous performance and failure issues: One of the side effects of the previous technology using PEAP was that it was user based and not computer based. Because there was no computer authentication taking place a laptop could not run non-user scripts. This resulted in numerous problems including failure to get mapped drives and printers as well as slow Authentication when returning from "Stand-By". By switching to a Certificate for both the Computer and User using a low cost internal Certificate Service we have:
 - ⇒ Resolved the user mapped drive and printer issues.
 - ⇒ Increased wireless Authentication performance.

\$708,402 Long Term Benefits or Payback: Anticipated, estimated multi-year benefits/ROI

- \$373,152 Configuration Savings & Certificate Savings for an additional 2617 users and 2676 laptops in 2009: As we grow our internal Wireless network and continue

embedding certificates in refreshed laptops we expect that all 5,000 existing laptops and their users will benefit from improved secure wireless thus avoiding configuration and certificate costs.

- ⇒ \$76,692 savings in configuration costs ($5000 - 2676 = 2324 \times \$66 / \text{hr} \times 0.5 / \text{hr}$)
- ⇒ \$139,440 annual computer certificate cost ($5000 - 2676 = 2324 \times \$20 / \text{yr} \times 3 \text{ years}$)
- ⇒ \$157,020 annual user certificate cost ($5000 - 2383 = 2617 \times \$20 / \text{yr} \times 3 \text{ years}$)
- **\$305,520 Multi-Year ROI:** When calculating the ROI an additional cost saving of \$567,000 is realized. As the desktop switch to laptops grows from 5,000 to 7,500 over the next 3 years the avoided costs will continue to increase.
 - ⇒ \$150,000 computer certificate cost ROI ($2500 \times \$20 / \text{yr} \times 3 \text{ years}$)
 - ⇒ \$150,000 user certificate cost ROI ($2500 \times \$20 / \text{yr} \times 3 \text{ years}$)
 - ⇒ \$5,250 RADIUS server and Certificate Authority (CA) Servers (Root, Polity & Issuing) certificate cost ROI ($\$350 / \text{yr} \times 5 \text{ servers} \times 3 \text{ years}$)
- **\$30,000 Cost avoidance data Multi-Year ROI:** We researched the approach used by other states such as Illinois and opted to avoid the \$15,000 cost of a commercial Certificate Authority and the 20% annual maintenance.
 - ⇒ \$15,000 Commercial Software Cost: Certificate Authority (CA) Servers (Root, Polity & Issuing) commercial software cost ($\$5,000 \times 3 \text{ CA servers} = \$15,000$)
 - ⇒ \$15,000 Commercial Software Annual Maintenance Cost: Certificate Authority (CA) Servers (Root, Polity & Issuing) ($\$5,000 \times 20\% = \$1,000 \times 3 \text{ servers} \times 5 \text{ yrs}$)

Additional Benefits:

- **Improved system availability (i.e. 24x7 access):** The previous computer password authentication required renewal every 30 days. The certificate authentication eliminates the need for renewal.
- **Reduction of duplicative efforts:** The enterprise certificate services architecture will provide a reduction in financial costs in that it will eliminate acquiring separate certificate services for each application. As security needs arise for state agencies, agencies will have an immediate, ready-to-use solution and will not need to build separate solutions.
- **Reduction of support staff:** Creating one enterprise solution decreases staff needed to support and maintain multiple applications.
- **Increased Security:** The enterprise certificate services provides increased security for information exchange for users of state services and lays the foundation to provide increased security for information exchange with federal and business partners and the public.
- **Increased Confidence in Security:** Providing an enterprise solution built to meet Federal Certification X.509 standards leads to increased confidence in the State's ability to protect data, provide secure information exchange, and reduce the risk of security breaches.
- **Consistent Application of Policy across State Government:** The Certification Policies and Practices Statement governed by representatives across State government ensure that policies and procedures are applied uniformly throughout the enterprise.
- **Single Identity for State of Maine Government:** The enterprise certificate services ensure one identity for the State of Maine employees and contractors.