

2002 NASCIO Recognition Program Nomination
for Outstanding Achievement in the Field of Information Technology

Title of Nomination: Transact Washington™
Project/System Manager: Lance Calisch
Job Title: Senior Project Manager
Agency: Washington State Department of Information Services
Address: 1110 Jefferson Street S.E., Mailstop 42445
City: Olympia
State: Washington
Zip: 98504-2445
Phone: 360-902-3440
Fax: 360-586-8992
Email: LanceC@dis.wa.gov

Category for Judging: Security and Business Continuity
Person nominating: Stuart McKee
Job Title: Director, Department of Information Services
Address: 1110 Jefferson Street S.E., Mailstop 42445
City: Olympia
State: Washington
Zip: 98504-2445
Phone: 360-902-3500
Fax: 360-664-0733
Email: StuartM@dis.wa.gov

Executive Summary

In December 2000, the Department of Information Services (DIS) launched its new secure portal, ***Transact Washington™***. Transact Washington is the state's authentication gateway for secure government services, designed to provide the state's trading partners with an entirely new way to do business with their government. Transact Washington is an extension of the state's Internet portal, ***Access Washington*** and leverages Public Key Infrastructure (PKI) and digital certificate technology to provide single sign-on access to numerous secure services offered by multiple state agencies. Using a single digital certificate, customers can go online to securely maintain records, access patient-identifiable information, fulfill reporting requirements or file taxes, all in a single Internet session conducted any time, from anywhere.

As part of the state's shared, secure infrastructure, Transact Washington can be used by any Washington public agency to transact business with trading partners. Built to comply with the state's security policies and standards, Transact Washington saves time and money by leveraging an optimum blend of state ownership and private sector expertise to eliminate duplication of effort, free up state resources and minimize secure application development time.

Security and trust are at the forefront of every government transaction. Transact Washington relies on digital certificates issued under the state's certificate policy to provide the means by which even the most confidential information can be accessed over the Internet. These certificates, issued by an outsourced trusted third party, provide levels of identity assurance not possible with user IDs and passwords. The high levels of trust and security provided by PKI and digital certificates means that the same electronic credential can be relied upon by a range of applications, both those currently in service and those yet to be offered.

Transact Washington allows new or existing applications to be easily incorporated into the Transact Washington environment, while providing agencies with a high degree of autonomy and control over their applications and who can access them. Transact Washington eliminates the need for agencies to build and maintain their own secure infrastructure, conduct the identification and authentication process, or PKI-enable their applications. As a result, agencies can concentrate on the critical business aspects of their applications, which results in quicker time-to-market and more responsive government.

Transact Washington was designed not only to enhance the levels of trust and security required by many of the state's emerging Internet applications, but to also to address Governor Gary Locke's mandate to "create a single face of government." Transact Washington provides one place on the Internet where state customers can use a single electronic credential to conduct business with multiple state agencies, which means it is no longer necessary to know which agencies provide the specific services customers need. Taking this concept a step further, Washington recently successfully piloted the use of its certificates with the Social Security Administration, opening the door for truly seamless transactions with all levels of government.

A. Description of the project, including length of time in operation

The explosive build-out of the Internet in the late 1990's brought with it an expectation that information of any kind should be available over the Web around the clock. Corporations demonstrated that a single portal could provide seamless, customized access to virtually any product or service they offered, and it quickly became apparent that Washington state's technically literate citizens expected no less of their government.

While the state was well underway with the deployment of its anonymous access information portal *Access Washington*, applying the same kinds of customer-driven requirements to allow access to secure information presented an entirely different set of challenges. The traditional security mandate of "keeping everybody out" had to be changed to "allowing the right people in." State security policies, which previously focused only on dedicated mainframe or LAN-based systems, needed to be reformulated to address the inherently greater risks associated with Internet-based access. Feeling pressure from citizens, state agencies scrambled to stand up dedicated, stove-piped security infrastructures to meet the requirements of their specific applications. The authentication methods used to identify known, trusted individuals were not strong enough or scalable enough to meet the security and confidentiality requirements necessary to provide access to sensitive data, offered by multiple agencies, to external trading partners over the Web.

DIS, in partnership with the state agency community, pulled together interrelated teams to develop a single, secure Internet portal. The teams developed and adopted policies, standards and guidelines needed to protect sensitive data and confidential business transactions over the Internet. These policies addressed the prevention of unauthorized data access, misuse of data, risk analysis and the need for stronger authentication requirements. The teams identified the business objectives for a scalable, reusable, enterprise security infrastructure, analyzed shortcomings in the existing infrastructure, and developed an architectural "road map" that outlined what steps were necessary to close the gap.

DIS was already in the process of enabling electronic transformation of paper-based processes through the use of digital signatures. The state realized that digital certificates and PKI -- the framework of legal and policy driven practices and processes necessary to create legally binding digital signatures -- could be effectively leveraged to provide strong authentication for users accessing data over the Internet. Further, a digital certificate, issued under a strong, trustworthy policy, could satisfy authentication requirements for access to even the most sensitive data, and the same trusted certificate, unlike a user ID and password issued to grant access to a single application, could be used by multiple application owners in multiple agencies.

DIS recognized that the infrastructure's administrative overhead and liability would be costly, and that the best solution balanced the need for control and ownership by the state with the efficiencies, expertise and core-competencies of the private sector. The project team recommended that the state own the applications, the physical security infrastructure and authentication policies, but would rely on the private sector, under contract, to provide PKI infrastructure services and customized help desk support for Transact Washington and resident agency applications.

Transact Washington, in production since December 2000, represents the convergence of these business and customer service-driven security initiatives in a single, secure Internet portal. Using a digital certificate issued by Digital Signature Trust under the state's certificate policy, citizens can go to one place on the Web to securely conduct business with many public agency applications in a single session. State or local government agencies can quickly get their applications up and running behind Transact Washington with the confidence that they are complying with the state's Internet access security policies and effectively leveraging the economies derived from a centrally managed infrastructure.

B. Significance to the improvement of the operation of government

Particularly within the context of data security, public sector agencies have traditionally relied upon specialized, proprietary processes and infrastructures to protect their information assets. This results in operational redundancy, duplication of cost and effort, and confusion and frustration on the part of authorized users attempting to gain access to this information. Additionally, to take economic advantage of the Internet, more trustworthy methods of user authentication need to be utilized. Transact Washington is a shared, enterprise level security infrastructure that provides enhanced levels of security and assurance while driving out the duplication of cost and effort created by individual, stove-piped security systems.

Transact Washington provides application owners with a high degree of autonomy and control over the content of their applications and who will be allowed access to them. Public agencies can rely on community-defined policies and a robust, scalable, security infrastructure to get their applications to market quickly. Transact Washington provides application owners with a comprehensive set of templates to register their application with Transact Washington and qualify users seeking access to their applications(s). Application owners can use an intranet-based facility to independently add and delete users and maintain their applications. By leveraging this “build-it-once” architecture, the state minimizes the time, technical resources, hardware and software costs and administrative overhead required to make secure applications available over the Internet.

Identity management is vital to providing an organization with a secure and scalable security infrastructure, as it provides the foundation for other critical activities such as access control and audit. Having greater assurance that the person requesting access is who they claim to be reduces the risk of unauthorized access, and means that that person can be granted access to applications containing more sensitive data. User IDs and passwords, traditionally issued by an individual application owner to grant access only to that application, are more prone to theft because they are passed over the Internet or stored on a central server. These proprietary credentials are rarely, if ever trusted outside the domain of the application for which they were intended, and are therefore not scalable across an enterprise.

Transact Washington relies on digital certificates, centrally issued under a certificate policy owned by the state, to provide a end-user authentication. This certificate policy incorporates best practices from many Federal policies, and invokes the prescribed processes and protections of the state’s Electronic Authentication Act to generate digital certificates that can be used with a high degree of assurance. The cryptographic properties of PKI ensure that a user’s identity is never passed over the Internet or stored on a central server where it can be compromised. This strong combination of identity management policy and technology means that, for the first time, very confidential data such as patient-identifiable information can be securely accessed over the Internet. Because this policy is trusted throughout the enterprise, a single certificate can be used to access multiple applications across multiple agencies.

Application owners no longer need be involved in the issuance or maintenance of identity credentials. Both internal and external users go to the same Web site to obtain a certificate. Digital Signature Trust, under contract with the state, handles all application, registration, identification, authentication and certificate life-cycle functions, and issues certificates conforming to the state’s certificate policy. Agencies are relieved of the cost and burden of having to personally authenticate individuals and perform password maintenance and resets.

To reduce the cost of staffing and overhead associated with application support, DIS contracts Transact Washington online support and help desk services to SafeHarbor Technology Corporation. State and local agencies also can take advantage of this state master contract.

C. Benefits realized by service recipients, taxpayers, agency or state

Transact Washington provides a secure Internet portal that generates value on both sides of the transaction equation. Public agencies can take advantage of Transact Washington's highly secure technology infrastructure, community-defined standards and common look-and-feel to quickly deploy applications behind a single authentication gateway. To eliminate the time, complexity and confusion required to maintain multiple User IDs and passwords for each application, trading partners need only obtain a single digital certificate that will be honored by all applications they have been granted access to. As a result, agency customers can by-pass several layers of bureaucracy by going to a single Web site to access a number of secure applications at their convenience, 24 hours a day.

Benefits realized by service recipients:

With Transact Washington, trading partners can now:

- Use a single electronic credential, rather than multiple User I.D.s and passwords to transact business with their government
- Conduct business with the state at their convenience, around the clock from their desktop
- Bookmark their own customized "MyTransact" Web page that provides a personalized list of the secure applications to which they have been granted access
- Save time by accessing information that previously took days or weeks to obtain through the mail
- Save money by eliminating the need for administrative staff required to place phone calls, submit information requests and process correspondence
- Increase business volume by reducing transaction cycle-time, providing more opportunities to serve more customers
- In the future, link from Transact Washington and use their Washington state digital certificates to access secure Federal applications over the Internet.

Benefits realized by public agencies:

By taking advantage of Transact Washington's policy-driven, shared infrastructure, Washington state and local government agencies can:

- Generate savings for individual agencies and economies of scale for the state by reducing overall business operating costs
- Leverage the speed, availability and cost-savings of the Internet to provide secure transaction capabilities to their customers
- Provide more responsive service to their customers and clients through timely access to information
- Concentrate on their critical business priorities, without having to stand-up their own security infrastructure, resulting in more responsive government and quicker time-to-market.
- Take advantage of increased business efficiencies by eliminating paper copy follow-up to online transactions
- Reduce transaction cycle-times and operating expenses by replacing paper-based systems with electronic processes
- Allow highly confidential information to be securely accessed over the Internet, including medical records and health information
- Leverage all the security and protections that come with digital certificates without having to PKI-enable their applications or install special software on their servers.
- Rely on a trusted third party to perform all user identification and authentication processes, thereby reducing the agency's liability and saving staff time.
- Maintain autonomous control of their applications while relying on a separately managed gateway to satisfy their authentication requirements.
- Comply with the state's Information Technology Security Standards
- Use Washington state digital certificates to transact with their Federal counterparts

Benefits realized by the taxpayer:

The primary benefit to the taxpayer comes from the elimination of duplicate cost and effort that would otherwise be required by individual agencies wanting to make secure information available over the Internet. Secure hardware and software costs, both for the initial deployment of a service, as well as those ongoing costs attributable to

upgrade and obsolescence are drastically reduced. Costs attributable to end-user authentication and password issue and re-sets are eliminated. Agency help desk staffing and training costs can be outsourced to further reduce state staffing levels and expenses. Transact Washington customers, who are also taxpayers, derive the benefits of being able to transact seamlessly with multiple agencies over the Internet, saving them time, money and frustration.

D. Return on investment, short-term/long-term payback (include summary calculations). Projects must exhibit measurable operational benefit.

For services such as the Transact Washington secured gateway, the return on investment is measured through applications deployed, service to the citizen and security and trust.

The metrics of success are not measured through the application itself but rather through the applications that use it. By building the secure Transact Washington key infrastructure once, agencies can connect applications into the structure without needing to recreate it for each agency or every new application that is deployed. To date, 13 applications have been deployed behind the Transact Washington secured gateway, with nearly 3,000 digital certificates issued. More are on the way.

The primary return on investment is to the businesses and citizens of Washington. In those cases where confidential information is required, no previous technologies were available to guarantee confidential and private transactions with highly authenticated partners over the Internet. Now, trading partners have a single sign-on gateway to conduct secured transactions with their government. This saves users time and provides a citizen-centric delivery of government services.

Security and trust are at the forefront of every government transaction. A digital certificate helps establish this trust, reduces the state's service delivery costs and makes the availability of entirely new classes of electronic transactions possible. Return on investment for both the state and its trading partners include greater operational efficiencies, reduction in administrative staffing, a reduction in paper-based processes and reduced transaction cycle times and expenses. Digital certificates can now be used to electronically file state business taxes, file workers' compensation claims, and provide and access HIPAA-related health information. Direct access to this data helps companies control workers' compensation costs and helps get injured workers the services they need and to return to employment.

As security and privacy requirements become more critical, costs for supporting interconnected networks and databases escalate. With Transact Washington, cost savings are realized by reducing the need for agencies to build separate infrastructures to support each agency's particular service. Application time-to-market is reduced, freeing up agency staff to focus on service delivery to the citizen, not on the development of security infrastructure.