



Entrust
Securing Digital Identities
& Information

Southwest Border States Anti-Drug Information System

Improving Homeland Security Through Law Enforcement Information Sharing

Putting the right information in law enforcement agents' hands is crucial to keeping borders secure and combating drug trafficking and other crimes. Since 1997, the Southwest Border States Anti-Drug Information System (SWBSADIS) has been enabling secure information sharing among law enforcement agencies in the Southwest states and with Federal law enforcement agencies. The SWBSADIS uses Entrust security to strongly authenticate users, encrypt data and e-mails, and digitally sign documents and communications.

Built by the Criminal Information Sharing Alliance, the system has been so successful that it has been expanded to include data sharing regarding money laundering, weapons, sex offenders, missing persons, criminal histories and other homeland security data. By eliminating prohibitive information silos, the SWBSADIS enables an integrated, secure exchange of information among federal, regional, state and local law enforcement agencies.

The Need

Inter-State Secure Information Sharing

The US border with Mexico spans 1,933 miles and the flow of drugs across the southwestern border crosses multiple law enforcement jurisdictional boundaries. Prior to SWBSADIS, California, Arizona, New Mexico and Texas each had their own separately operating criminal information systems. Disparate computer systems, inconsistent security policies, privacy restrictions, interoperability hurdles, conflicting governing regulations and high costs often made the sharing of vital information impossible.

It was imperative for law enforcement officials to be able to securely share information on the criminal activities of drug offenders regardless of state lines and jurisdictions. SWBSADIS was created to overcome these barriers and give law enforcement officials a vital tool for their fight in the war on drugs. The four border states requested and received funding for the SWBSADIS project from the Department of Defense, and the system became operational in 1997.

The Challenge

A Security Framework Spanning Multiple Systems

The SWBADIS security framework protects the confidentiality and integrity of information, identifies and authenticates participants, and enables remote access and offline use of sensitive information. Since each state operates its own information systems, the security framework linking them together had to be based on proven technologies that could interoperate with a variety of platforms and applications. Additionally, the overall system had to be cost-efficient and effective.

The Solution

Securing Communications and Access to Data

To meet this challenge, the Criminal Information Sharing Alliance chose Entrust technology for the SWBSADIS security framework. Using Entrust software, agents and law enforcement officials can sign and encrypt messages so that the computer network can identify the credentials of legitimate users, determine which resources they are allowed to access, and protect their documents and transactions.

Not only does the SWBSADIS network provide the basis for establishing and maintaining a trustworthy networking environment, but it also accommodates large volumes of users and interoperates with numerous commercial software applications. In addition, it enables the law enforcement agencies to manage security and privileges automatically, and revoke or suspend them if an authorized user's job status changes. Because this solution embraces open standards, is based on proven technology and is interoperable with a wide variety of platforms and applications, it has been very successful and is a good model for other law enforcement needs.

"Since this project crosses jurisdictional lines, we needed a proven technology that everyone agreed was secure enough to protect highly sensitive information. We chose Entrust because they provided the best-of-breed technology and the flexibility required to bridge our participants' disparate systems."

Glen Gillum, Director, Criminal Information Sharing Alliance

The Benefits

Entrust technology has helped meet SWBADIS's key objectives for their security framework: critical infrastructure protection and new business process enablement. For SWBADIS, critical infrastructure protection means identification and authentication of users, and confidentiality, integrity and availability of information assets. New business process enablement is the flexibility to take advantage of new technologies to facilitate better and more efficient work processes, such as agent remote access and electronic workflow management.

The SWBADIS enables law enforcement agents to take advantage of numerous applications, including secure messaging and e-mail, secure web access, secure electronic transactions, secure desktops, secure virtual private networks, secure electronic documents, and single sign-on. These applications allow them to use existing systems to identify others with similar investigative interests and to rapidly and securely exchange sensitive intelligence and other investigative information. Each transaction can be encrypted and digitally signed, enabling user authentication (valid user credentials), authorization (access control), confidentiality (privacy), integrity, non-repudiation and availability.

The Future

Efforts are underway to expand the SWBSADIS model to other state and local regions and to integrate its applications with federal databases, such as the US Department of Justice CopLink and the Immigration and Naturalization Service. Providing a secure information-sharing network among authorized government and law enforcement officials at multiple levels will facilitate critical, real-time access to information needed to enhance America's homeland security. By eliminating information silos and improving information security, it allows for exactly the kind of integrated, protected exchange of information required to win the war against terrorism.