DIGITAL SECURITY INITIATIVE
CASE STUDY

Smart Card Alliance

California ISO secures access to electric power grid controls with smart cards and PKI

In 1996, California lawmakers enacted historic legislation allowing consumers to choose their energy suppliers in order to create a competitive marketplace for public utilities. The California Legislature conceived the not-for-profit, public benefit organization, the California Independent System Operator (California ISO), to manage the power transmission grid and to facilitate markets for electricity reliability products. Created by PG&E, Union Gas and Electric, and Southern California Edison, they are the air traffic controller of the electrical grid. They oversee the path, routing and sale of energy across 80 percent of the grid of California.

The power grid, a transmission system made up of high-voltage power lines, delivers enough power to serve the annual energy needs of over 30 million current customers of investor-owned utilities. In addition, the grid will transport significant amounts of power for others in the region.

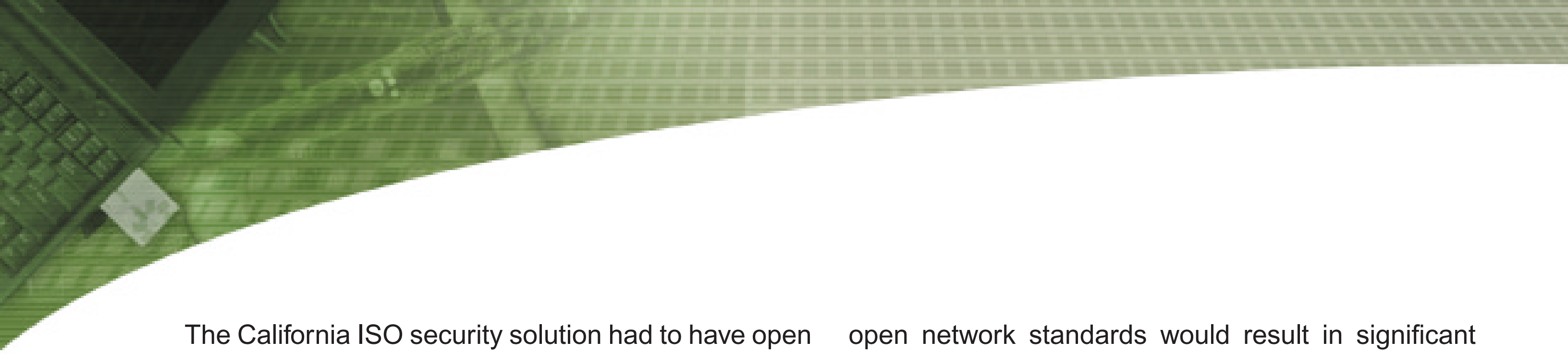
In 1996 the California ISO created a specialized team whose task was to define their information security requirements. The resulting plan was required in order to satisfy Federally mandated tariffs that defined the business requirements regarding a PKI deployment. The Cryptographic Universal Design Architecture (CUDA-ISO™) team was created. The CUDA-ISO™ team spent two years of research, due diligence, policy development, and security architecture development before the deployment of the PKI and smart cards began. By 1998, the overall security architecture, PKI policy and practice statements, subscriber requirements, and subscriber education and training deliverables were complete.

To deploy their newly defined security plan, California ISO chose SPYRUS Inc. to provide the PKI, Rosetta™ smart cards, and the LYNKS™ high assurance cryptographic tokens to satisfy these information security requirements. In the spring of 1999, the California ISO began to deploy their PKI and issue smart cards to their user base. To date nearly 2000 California ISO smart cards have been issued.

PROJECT OVERVIEW

The California ISO was created to monitor power generation facilities, manage the transmission grid, manage the buying and selling of electricity, and provide the e-business framework necessary to ensure commercial equity across business areas. A specialized organization was created and chartered with architecting, developing and deploying a secure information framework that could accommodate the varying levels in information assurance required to operate the diverse components of their business.

Energy systems are a National Critical Infrastructure component, and the development of a comprehensive security package for protection of physical and logical assets is essential. California ISO assembled a team to implement the network's firewall security and to plan security for the network's eventual move from a dedicated private network to the Internet. During the next 15 months, the CUDA-ISO‰ team developed criteria, selected vendors, and began to deploy a master security solution across the California ISO network.



The California ISO security solution had to have open standards and be non-proprietary. The CUDA-ISO™ team identified confidentiality, ease of use, scalability, and a life expectancy of at least ten years as the essential system requirements. Confidentiality was vital because unauthorized access to privileged trading information could give an unfair advantage to energy auction participants. Ease of use was essential to California ISO's many and diverse clients, including utility, generator and transmission companies and energy traders. Scalability of the on line security system was essential to accommodate additional electrical generating plants and traders over time.

Charged with managing the power transmission grid and coordinating the flow of electricity throughout the state, California ISO quickly recognized its critical need for a high-assurance security infrastructure. The California ISO system is currently operational across a number of different applications. High-assurance applications including power generation use high capacity PCMCIA hardware tokens, medium-assurance applications such as secure scheduling and dispatch operations use smart cards, and basic-assurance services including invoice submission utilize browser software certificates. This combination of secure tokens are utilized to provide a robust and comprehensive security solution.

California ISO began to deploy their PKI infrastructure and issue end user smart cards in March 1999.

PROJECT BACKGROUND

When the California energy market was broken up and the California ISO created, a "clean slate" was provided upon which to create a new operating environment. State of the art technology was selected to satisfy the many requirements defined by several factors. Newly defined tariffs defined rules for information confidentiality, liability, indemnification, and dispute resolution. Existing control networks were predominantly leased line networks, and the move to open network standards would result in significant costs savings. There was the need to remove barriers to market participants. If future trading of transmission rights were to include different players, those organizations would have had to install dedicated lines connecting them to the California ISO networks. These tremendous barriers to participation would need to be resolved by implementing a secure system that could provide highly secure, authenticated access.

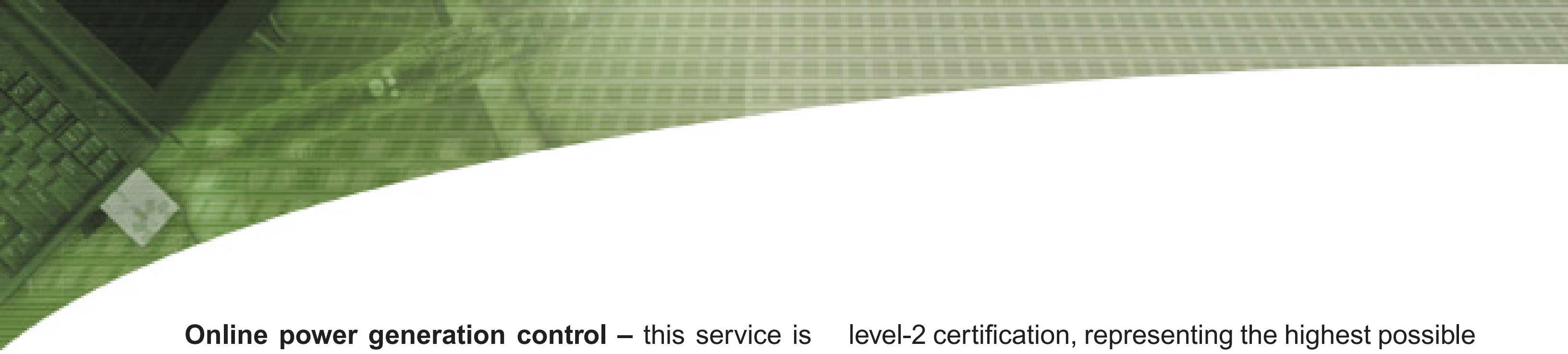
APPLICATION DESCRIPTION

When California ISO became operational, the network consisted of a statewide virtual private network (VPN) that ran Internet Protocol (IP) over dedicated lease lines. California ISO assembled a team to implement the network's firewall security and to plan security for the network's eventual move from a dedicated private network to the Internet, which would lower costs and allow for easier system expansion. To reduce the cost of expensive dedicated leased lines, California ISO wanted to use the Internet wherever feasible.

The California ISO PKI deployment supports multiple levels of assurance. The high assurance system operates the power generation and transmission grid facilities. These systems utilize a high assurance PCMCIA token to support the cryptographic functions. The medium assurance systems support the various trading and metering applications, and utilize smart cards. Basic assurance systems use software certificates to manage basic information flows.

In enabling business to operate in open network environments, the power entity successfully implemented a number of secure e-business applications, including the following:

Online trading - over an extended Internet/Extranet network, buyers and sellers of power are authenticated to access an online auction of transmission rights through use of software certificates.



Online power generation control – this service is secured through use of high-assurance LYNKS™ Privacy Cards.

Online meter access – access is secured while enabling online meter access by third parties of the kilowatts supplied to customers throughout the transmission system.

Online invoicing submission - access is secured using a web based certificate.

Online problem management - smart cards are used to secure remote access while tracking problem resolution quickly and efficiently. More than 500 California ISO users also utilize smart cards to secure online network load balancing, supporting real-time power trading services to cover spot imbalances of power.

Scheduling notification - another smart card based application, automatically alerts electric generation facilities to outstanding bids to purchase energy and prompts them to respond to the request. By responding, the facility commits to produce a specific number of kilowatts of electricity. This step guarantees that electric generation plants across the state have the opportunity to compete fairly in the open market.

Around California, more than 800 scheduling coordinators use their smart cards to conduct their transactions with the California ISO. The CUDA-ISO™ team implemented an Internet-enabled application that allows participants to securely manage the bid submission process online.

All of the applications are securely managed by the PKI, comprising four Certification Authorities (CAs) and two Registration Authorities (RAs), with additional expansion planned at all levels within the network. The smart cards deployed in the California ISO system are SPYRUS Rosetta‰ smart cards. These cards are 16K crypto-controller smart cards running the SPYRUS SPYCOS™ chip operating system. These highly secure smart cards have received the Federal Information Processing standard (FIPS) level-2 certification, representing the highest possible security level available for smart cards today.

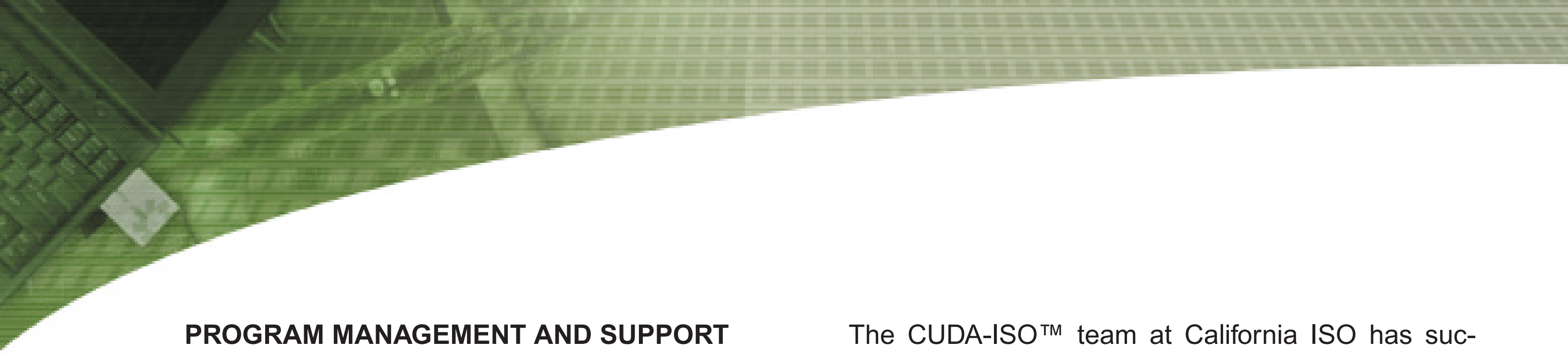
IMPLEMENTATION OVERVIEW

In 1997, Cal ISO began to construct a private ATM network secured with state of the art firewall technology. This network would provide the backbone upon which all Cal-ISO business would be conducted. Authentication was to the network, and once an end user gained access to the network, all resources became available. All of the newly developed energy management systems, and marketing databases would tie control of the grid to the market, and all of these systems operated on a single private line network.

By 1998, once the initial backbone was in place and operational, Cal-ISO began the task of conceptualizing a new approach that would support higher levels of security, reduce network costs significantly, and be able to scale in functional capability as well as numbers of users supported. In addition, criteria for the new capabilities had to follow open standards, be non-proprietary, and sustain long life spans.

An RFI was issued to collect inputs, and the verdict that followed reflected that a PKI would be the only solution that could meet all of the requirements. Multiple RFPs and RFQs were issued, and the final team selection process finally occurred in January of 1999.

The CUDA-ISO™ team managed the entire process. Final partner selection resulted in SPYRUS providing the PKI and hardware tokens, and SAIC was selected to be their integrator. By March of 1999, work to build the California ISO PKI had begun, and within six months, three Certification Authorities running separate policies had been stood up, and smart cards were being issued to end users. The CUDA-ISO™ team created a fourth certification authority, allowing them to test new security releases before releasing them to the field.



PROGRAM MANAGEMENT AND SUPPORT

The Cal ISO deployment was managed entirely by Cal ISO. SAIC provided the development and integration support services necessary to bring the applications online. A client support services organization was created within Cal ISO to provide the help desk, trouble ticket generator, and problem management functions. The Remedy database provided a web-based tool that was accessible by end users who, by using their smart card, could track the status of disputes, network connectivity issues, or any other network, user, or business issue involving the new Cal ISO systems. Training was provided by internal organizations and web-based information systems supplied additional reference data to end users.

Smart card issuance involved in-person registration authorities that performed the checks necessary to ensure the identity of the recipients of the digital credentials. In the event a card was lost or stolen, certificate revocation and credential (smart card) re-issue processes ensured workflow disruption was kept to a minimum.

COSTS BENEFIT ANALYSIS

It is a gigantic task for California ISO to securely manage the generation and sale of $50-100 million each day in electrical energy. From its headquarters in Folsom, near Sacramento, California ISO's automated command and control network regulates the generation and metering of power from remote generators located throughout California.

The CUDA-ISO‰ team's initial efforts concentrated on defining California ISO's security architecture and application requirements and then implementing a VPN with proxy management. The flexibility of the deployed security policy has enabled California ISO to develop and deploy network applications rapidly. All future California ISO applications must conform to CUDA-ISO‰ specifications and will migrate to the new security policy.

The CUDA-ISO™ team at California ISO has successfully deployed a PKI infrastructure solution into a pre-existing critical infrastructure, enabling the organization to offer a broad range of services and add levels of security not previously available to the energy industry in California or anywhere else in the world.

E-business is a reality in today's marketplace. California ISO entered this new environment with the highest level of confidence, knowing that their mission-critical transactions would be tightly secured. Not only did the California ISO eliminate security concerns in a cost-effective manner, the solution also allowed them to implement innovative e-business applications that reduced operational costs.

The cost/benefit analysis would reflect that the deployed solution was the only viable alternative that would provide the necessary framework for network, information, and transaction security. In the end, Cal ISO realized significant savings through reduction of Cal ISO's dependence upon dedicated private line networks. In addition, the successful deployment of the PKI and smart cards allowed the CUDA-ISO™ team to completely eliminate a migratory step, one that entailed the deployment of a VPN utilizing authenticated proxies. This efficiency resulted in a costs savings of hundreds of thousands of dollars and many months. Web enabled security applications sped deployment schedules significantly as new online applications easily replicated the security architecture.

LESSONS LEARNED/RECOMMENDATIONS

Deploying state of the art technology requires extreme diligence on behalf of the owning organization. The fact that Cal ISO spent over a year investigating the alternatives in technology is testament to this fact. It is extremely important that the deployed technology meet the operational requirements of the system.

Fully architecting a security solution as an ENTIRE system is critical. An effective security solution cannot be an assembly of numerous components that may or may not adhere to a unified policy. This architecture must also be supported by the requisite Certificate Policies and Certificate Practice Statements.

Scalability is also an important factor. Scalability must be viewed as the number of objects supported by the system. Usability for the different types of certificates, including the smart card form factor, is another key element that needs to be considered when deploying security solutions. Very often, issues surrounding scalability and usability are closely related.

One time provisioning was also a key element of success in the Cal ISO deployment. The security team did not have the luxury of a second chance. Once deployed, the security architecture had to work.

Finally, performance and application impact were categories that required considerable diligence in the planning cycles. System performance impacts had to be kept to a minimum, user interfaces to applications had to reflect little or no change, and deployment transparency became a key objective.

By employing personnel possessing considerable expertise, conducting a thorough due diligence cycle, exercising a complete RFI/RFP/RFQ cycle, and applying sound program management principles, California ISO was able to meet their objectives in enabling the new California energy marketplace to confidently conduct business within a new security framework.

Rosetta™ and LYNKS™ are trademarks of SPYRUS Inc. CUDA-ISO™ is a trademark of the California Independent System Operator.

This case study was developed by the Smart Card Alliance's Digital Security Initiative
with the assistance of Bryan Ichikawa and Spyrus Inc.
For more information on this and other case studies
or to obtain additional no-cost resources
on the use of smart cards in digital security,
contact the Alliance at www.smartcardalliance.org.