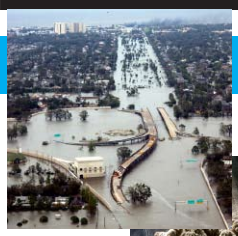
TRUSTED DATA SHARING

MEETING THE NEED FOR SECURE DATA SHARING

Sandia National Laboratories

SANDIA NATIONAL LABORATORIES

Lessons Learned



In times of crises, secure information sharing is vital to the safety and security of this nation.

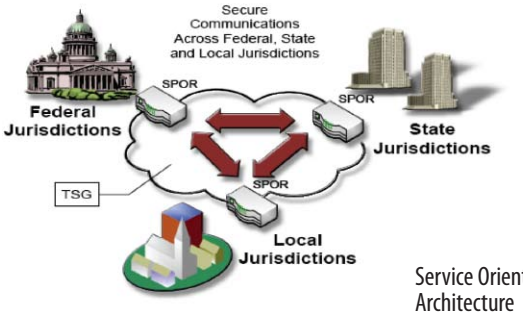
At Sandia National Laboratories, our Homeland Security and Defense work seeks to provide enduring contributions to secure our society against high-consequence terrorist threats and national incidents through the effective use of science, technology, and systems solutions.

In 2001, the unprecedented terrorist attack on an American city — New York City's World Trade Center — brought significant attention to cross-governmental communication needs and systems that provide authenticated alert and warning messages to the public.

Additionally, Hurricane Katrina taught us valuable lessons on the need to develop a communications system that would allow all involved agencies to stay in the know. Subsequently, Executive Orders 13356 and 13353 issued by the President required an improved ability to share critical information among the differing governmental agencies, and across federal, state, and local jurisdictions.

Research and Development Opportunity

In response, Sandia National Laboratories (SNL) and its experienced partners, have designed a demonstration technology—called Trusted Data Sharing Architecture—to meet the need for secure data sharing, especially during emergencies. Research and development is ongoing to refine this system-of-systems approach to provide secure, scalable, and interoperable data sharing within and among federal, state, local, and tribal agencies.



Service Oriented Architecture

Information Standards

One major reason why SNL is sought out by customers is due to its science-based, systems engineering approach to complex problems. The multifaceted issues surrounding secure cross-jurisdictional communication is another example of a complex problem requiring a standards based approach. SNL is heavily involved in ensuring standards are formulated and implemented in the Service Oriented Architecture (SOA) environment (information eco system). SNL is working with the Organization for the Advancement of Structured Information Standards (OASIS)* to drive the development, convergence, and adoption of open standards for SOA, among other things. OASIS represents more than 600 organizations and members from more than 100 countries.

Standards provide the following additional benefits:
- Potential for cost reduction
- Stimulation of innovation
- Growth to global markets
- Protection of the right of free choice of technology.

Advantages

Trusted Data Sharing Architecture offers six crucial data-sharing advances.

- **Security**— Messages are delivered only to intended recipients. Receivers are notified that an authorized sender has sent a message.
- **Interoperability**—Cross-enterprise operability provides secure transmission between multiple jurisdictions, agencies, and communities of interest.
- **Scalability**—Jurisdictions may be added to the recipients without creating multiple point-to-point links to their respective system.
- **Reliability**—Messages are sent by multiple channels that can reach identified destinations anywhere, anytime. Choreographed grid operation and management enables robust message routing for high-assurance message delivery.
- **Near Real-Time Information Sharing** — Event driven information sharing ensures the right information at the right time.
- **Geographically Targeted**—Tailoring where information is delivered via dynamic rule based routing.

* (http://www.oasis-open.org/home/index.php)

THE CHALLANGE

How do we simultaneously enable data security and selected accessibility?

In other words, how do we share critical data with entities that have an urgent need-to-know while protecting that information from adversaries?

Today, each jurisdictional agency—federal, state, and local—applies diverse and separate technical, policy, and security mechanisms.

The result: During emergencies, multiple independent entities are, in effect, blocked from secure communications with one another. Because a coordinated effort to control and manage shared information has not been developed—when the clock is ticking and seconds count—agencies run up against serious complications, including:

- Existing technologies for networked data sharing cannot effectively communicate through differing jurisdictional barriers.
- When networked communication is initiated between jurisdictions, the data usually becomes insecure.
- If two agencies do succeed in securely transmitting data, a third problem arises—scalability — when the necessity arises to add another recipient to the grid.

Especially during emergencies, it is critical to make secure information sharing easier. At home and on the battlefield, we know from experience that communication failures can lead to deadly consequences.

THE SOLUTION

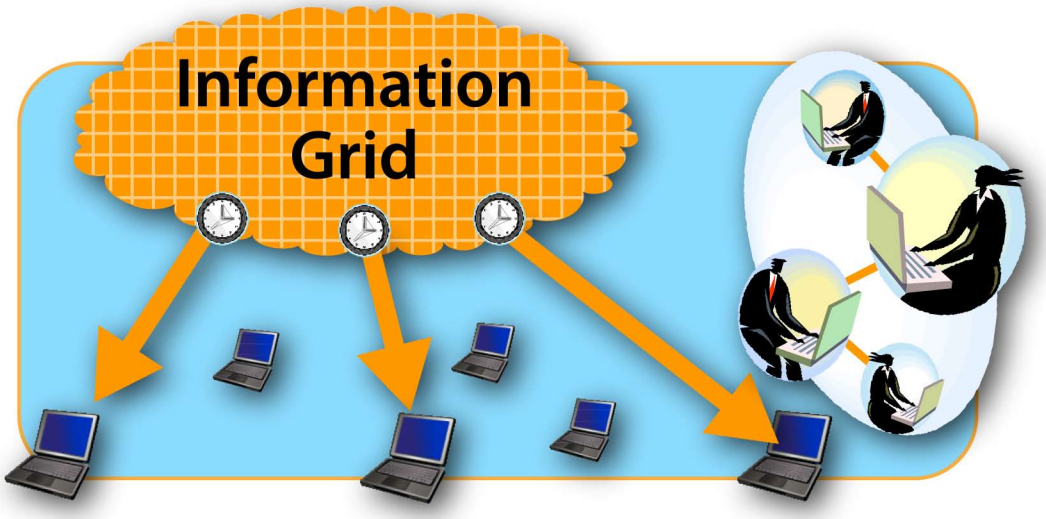
Span the Gap

Multiple organizations need a common approach for secure information sharing, yet a technology gap exists between data security and data access. To span the gap, SNL has partnered with industry to demonstrate a ***system-of-systems solution*** that provides secure data routing and communication across federal, state, and local jurisdictions, while at the same time improving business and industry cyber communication security.

Trusted Data Sharing Architecture ensures secure information sharing across and between agencies through features that address the following issues:

- Management of Last Mile Bandwidth limitations.
- Asynchronous vs. synchronous impact on scalability.
- Providing security, authorization and identity management
  - Providing non-repudiation security of need to know information
  - Intermittency concerns of reliability and connection.

SNL has evaluated possible solutions, and has concluded that SOA provides the best solution to cross-jurisdictional cyber communication. SOAs have been specifically designed to provide a solution to the cross-enterprise message-system integration problem while at the same time, addressing scalability.



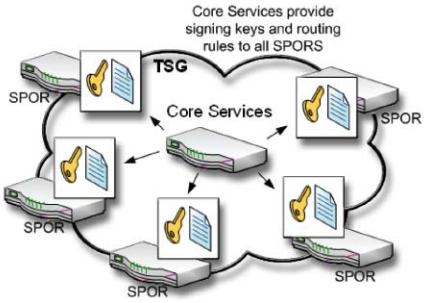
Getting the right information to the right place at the right time SECURELY

HOW IT WORKS

How Trusted Data Sharing Works:

Service Oriented Architecture. An SOA is a flexible, standardized software architecture that integrates systems to enable interoperability; in essence, a group of services that communicate with one another. SOAs are positioned to solve the cross-enterprise message-system integration problem while also providing scalability.

Core Services. These propagate policy, routing rules, and data protection information to all participating Secure Policy-oriented Object Routers (SPORs). After this core information is distributed, a message can be injected into a SPOR and routed to appropriate destinations.



Establishing a TSG grid.

Secure Policy-oriented Object Router (SPOR). After Core Services have distributed keys and policies to all participating SPORS in the grid, any SPOR in the grid can deliver a message using Emergency Data Exchange Language - Distribution Element (EDXL-DE) to send data through the Trans-Enterprise Services Grid (TSG). Messages are sent only to specified receivers. At the receiving SPOR, the message will bear the sender's identification for authentication.

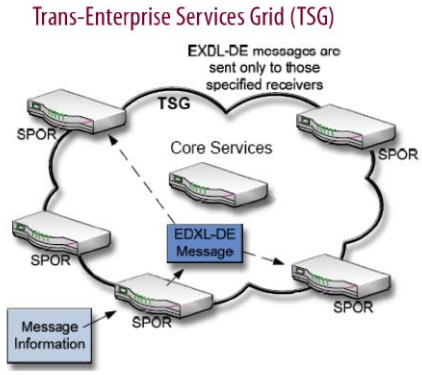
SPORs route information through the TSG. A framework for Trusted Data Sharing, SPORs provide:

- Secure, policy-oriented rule-based routing,
- Data protection,
- Open standards.

SPORs enable the secure transmission of information by using standards-based policy and routing rules. These policies and rules enable the system to:

- Identify the sender and receiver of a message,
- Specify what each is allowed to do with the message,
- Protect the message.

Communication between SPORs relies on Internet Protocol; SPORs provide a secure gateway between the jurisdiction's enterprise and the Internet. The TSG forms a secure information sharing Community-of-Interest (COI) partition from the internet as shown below.



The standards-based TSG implements the SOA.

Trans-Enterprise Services Grid (TSG). The TSG uses a data-centric processing flow model, whereby context, status, and security are kept with the message object itself. This removes unnecessary steps and simplifies the work done at particular process nodes in the system, thus, eliminating excess traffic. The TSG can wrap and unwrap context, provide security, and reduce processor overhead and traffic between nodes. The TSG uses standards developed by the Organization for the Advancement of Structured Information Standards (OASIS) (see discussion, page 1).

Unique TSG benefits include:

- **Nonrepudiated Message Admission.** This ensures the message was actually sent by the entity who claimed to send it.
- **Transfer of Trust.** As the message flows, the TSG can be trusted as the delegated information carrier.
- **State Encapsulation in the Message Data Object.** Additional routing, security, and policy information is carried with the message.

For More Information

Sandia National Laboratories welcomes partnerships and collaboration with federal agencies and other interested partners.

For more information regarding Trusted Data Sharing architecture, contact Chuck Oien, ctoien@sandia.gov, 925-294-2077.

Sandia National Laboratories

Sandia is a multi program laboratory operated by Sandia Corporation, a Lockheed Martin company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000. SAND 2008-8112 P