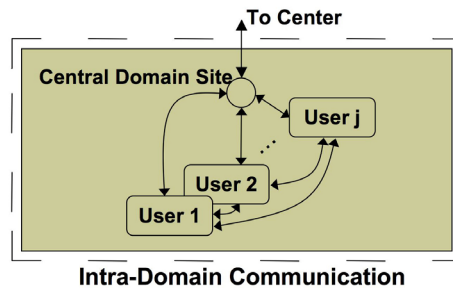
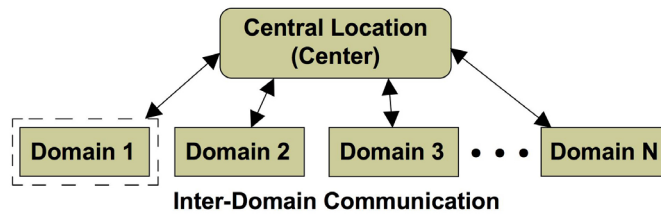




# Anonymous, Authenticated Communication

## Overview

Anonymous, Authenticated Communication (AAC) addresses the issues associated with providing anonymity to an authorized group of users (domains) who share digital information with a central collection/analysis/distribution center. Anonymous yet authenticated communication capabilities are desirable when users communicate with trusted entities, but wish their identity to be separate from any information they contribute. Our AAC system includes software that implements cryptographic protocols for anonymous authentication of messages. We also provide guidance on using existing technology for anonymous communication and message content anonymization. With our approach to cryptographic anonymity, the receiving center can ensure that an arriving message is from a member of the group, but neither the center nor an electronic eavesdropper can determine which member of the group sent the message. The AAC system is implemented in the I3P Cross Domain Information Sharing (CDIS) demonstration system.



*High level anonymous, authenticated communication model.*

### Why is Anonymous, Authenticated Communication Important?

Sharing of information within a user community is important in understanding threats and early detection of coordinated attacks, but anonymity and authentication of communication is crucial to maintaining trust in information sharing within the community. Sharing of meaningful information is often not worth the risk of identifying the source. Anonymous, authenticated communication is an enabling technology to secure sharing of critical infrastructure information.

### Key Concepts

Attributes of our Anonymous, Authenticated Communication system include

- Anonymity of the message author,
- Anonymous network communication paths,
- Authentication of the source,
- Anonymity and integrity of the data, and
- Protection against system abuse by insiders.

## Functional Description

Our AAC system involves three elements, described below: 1) Cryptographic protocols for anonymous authentication of shared information, 2) Anonymous communication of shared information, and 3) Anonymization of the content of shared information.

- **Cryptographic anonymization.** Cryptography-based anonymous authentication can facilitate information sharing through protection of identity and data. The receiving center can ensure that messages are from authorized members of the group, but the center or eavesdroppers cannot determine which member of the group sent the message. The sharing of sensitive information attributable to a particular user has risks that our cryptographic solution can mitigate. Since anonymous communication opens the door for untraceable system abuse by insiders, our approach to cryptographic anonymity employs message revocation (when warranted), yet retains true anonymity of the message sender.
- **Communication anonymization.** Cryptographic anonymous authentication is not sufficient for identity protection. An observer of the communication network might trace the path of information from the sending Domain to the Center. Therefore we need to anonymize network communication between senders and the Center.
- **Content anonymization.** The use of operational procedures and/or filtering techniques to anonymize or sanitize message content is an equally important element to any solution.

Refer to the following paper for a detailed discussion of anonymous, authenticated communication. T. Draelos, C. Eliopoulos, A. McIntyre, W. Neumann, R. Schroepfel, "Anonymous, Authenticated Communication for Secure Sharing of SCADA and Control System Information," in Proc. SCADA Security Scientific Symposium (S4), Miami, FL, Jan. 2007.

## Researcher Contact Information



**Tim Draelos**  
 tjdrael@sandia.gov  
 (505) 844-8698

## About Sandia National Laboratories

Sandia is a multiprogram 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

This work was supported under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College.

## Technical Description

The cryptographic protocols in our AAC system were developed and implemented by Sandia National Laboratories. Communication and content anonymization are important elements of our AAC system and can utilize existing technology. The technical description of these three elements is provided below. For communication and content anonymization, we list multiple options.

**Cryptographic anonymization.** The security of the cryptographic anonymization protocols is based on the fact that all users have the same key material, thereby ensuring anonymity within the group, yet authentication of group membership.

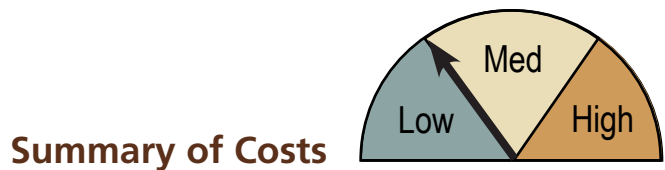
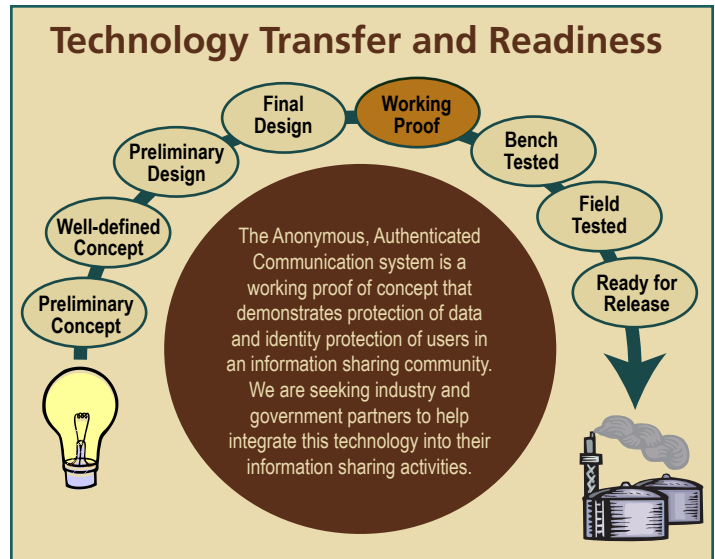
- *All domains use the same key material.* During initial setup, a hardware token with random numbers is acquired from the Center.
- *The key material changes daily to avoid proliferation.* The Center randomly generates and securely distributes a daily token.
- *New encryption and authentication keys are generated for each message.* The message sender encrypts and authenticates the message and sends it to the Center along with an index to the hardware token.
- *Decryption and authentication keys are regenerated for each message.* Using an index from the message sender, the decryption and authentication keys are regenerated from the common key material. The recipient can decrypt the message and verify that it came from an authentic user, but doesn't know which one.
- *The Center can revoke a message without revealing the sender's identity.* Revocation tokens can be used to revoke a message without revealing the message sender's identity.

**Communication anonymization.** The communication options are listed in order of weakest to strongest in terms of anonymity protection.

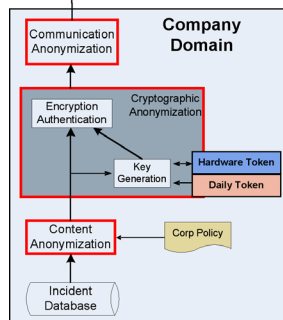
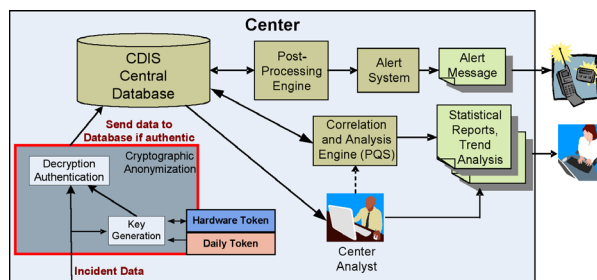
- Anonymous remailers (e.g., Simple, Mixmaster), Randomized proxy networks (e.g., Crowds)
  - Type 0 - Provides sender anonymity but no more
  - Type 1 - Provides sender anonymity and some sender/receiver-unlinkability
  - Type 2 - Greatly improves traffic analysis resilience; May offer reply e-mail services via pseudonyms and logging
- Onion routers (e.g., Tor)
  - Onion routers provide the strongest and most flexible anonymous communications
  - They are not enough for our needs since they provide no authentication

**Content anonymization.** Content anonymity options include manual and automated procedures to detect and prevent attempts (inadvertent or malicious) to release sensitive information that could result in compromised anonymity.

- Manual
  - Establish Clear Policies and Operational Procedures
  - Train users on how to implement policy
- Automated
  - Structured forms with no free-text
  - Information review and keyword filtering/modification
    - XML Stylesheets
  - Bayesian filtering



	Low	Medium	High
<b>Component</b>	<\$1,000	\$1,000-\$10,000	>\$10,000
<b>Engineering</b>	Drop-in	Moderate modification	Complete System Design Lifecycle
<b>Bandwidth/Network Burden</b>	None-Passive Only	Moderate Traffic, Medium Overhead	Heavy Traffic, Large Overhead
<b>Training</b>	No training required	Moderate training	Intensive training. Additional staffing may be required.
<b>Maintenance and Operation</b>	< 1 hour per week	< 5 hours per week	> 5 hours per week



**Anonymous, Authenticated Communication in a CDIS application.**