Comparisons of a distributed and centralized LRIT architectures
OR
The importance of technology neutral language in the IMO

Introduction

This describes a distributed secure scalable Long Range Identification and Tracking (LRIT) architecture. Relative to the centralized approach, a distributed approach simplifies many aspects of LRIT deployment, reduces cost, accelerates deployment and encourages innovation. At COMSAR 9, the Subcommittee agreed it was important to understand the various LRIT system architectures. Here is one such architecture.

Comparison of Centralized and Distributed LRIT Architectures

The following is a comparison between centralized and distributed approaches to LRIT implementation. It shows the benefits of distributed architectures in security, reliability, scalability, and costs.

Security
With an intermediary between the source of LRIT information and its final destination, the centralized approach creates an additional weak link in the chain. The central database, which may be outsourced, contains LRIT information from all tracking service providers (TSPs) and therefore holds information for all vessels. This creates a high value target for cyber attack or clandestine information gathering. Adding the additional stop between the TSP and the various LRIT listeners only weakens the security of the data by having it "in the clear" – decrypted at another point in the network. Mirroring the database may increase reliability but further weakens security by creating more high value targets.

In a distributed system, encrypted information moves directly from TSP to LRIT listener and offers no opportunity for the attacker to see or modify decrypted data. There is no centralized point with all ship locations and hence, nothing to attack. This distributed nature makes it all but impossible to shutdown the LRIT system since data paths are spread out amongst all TSPs which are geographically distributed and connected via different networks. Being able to function after a massive attack is what led to the same distributed design of the Internet.

Reliability
Regardless of how it is stored, adding a point where all TSP data must flow before reaching its destination creates a single point of failure. The reliability of the link for LRIT information from TSP to LRIT listener is not improved by adding an intermediate stop. Adding mirror nodes may improve the reliability of this "stop", but they still become points of failure. In a distributed system, the failure of any element still allows the rest of the system to function. This fault tolerance comes at no additional cost.

Scalability / Avoiding Obsolescence
Bandwidth - Due to the fact that all LRIT information must be disseminated from a single point (or a few mirror sites) to all entities in all States, in the centralized database architecture (CDBA), growth of the system is limited by the bandwidth of the communication link through the

centralized database (CDB) – a bandwidth bottleneck. Rough calculations[1] indicate approximately 28Mbps would be required to support the current number of vessels. However, should continued growth be asked of the system to support voluntary participation by all craft such as lifeboats and pleasure craft, the CDBA would quickly run into bandwidth limitations (requiring close to 500Mbps for a million vessels). However, for a distributed secure scalable architecture (DSSA) like the one described in this paper, this is not a concern as bandwidth requirements are divided across all TSPs based on their service and consequently their revenue levels[2].

Computational bottleneck – In the CDBA, calculations regarding ship position with respect to various coastal contours and distance off shore, as well as other compute-intensive tasks, must be done for all roughly 65000 SOLAS vessels – a computational bottleneck. Increasing the number of craft 10 or 100 fold may require the use of increasing numbers of computers. In a DSSA, since such calculations are already performed by TSPs, the computations are inherently distributed across TSPs, effectively forming a distributed or grid computer. This not only frees up computational resources but opens the door for the innovation of improvements and new features. Such an example may be the use of advanced algorithms to provide more accurate heading, position and velocity estimates between LRIT points with the incorporation of other information (like the expected port state[3]).

Build out costs, Time to Roll-Out, Personnel and operational costs

The centralized approach will require the determination and creation of funding mechanisms for the initial build-out, additional personnel (salary, benefits), facilities and the operational costs for maintaining the mirrored centralized database. This additional cost will have to be borne by the states. These and the possibility of an intergovernmental approval process are all items that inherently take time and may therefore delay LRIT deployment. However, in the distributed case, there is no requirement for funding by the states. The simple definition of a common interface specification between LRIT listeners and states sets the ball in motion.

As more TSPs become part of the LRIT service, costs to generate LRIT information in the correct format will be borne by the TSPs. In fact, it may behoove TSPs to provide the LRIT listener software as well as to any contracting governments or other end-users who do not have a system of their own already in place[4].

For purposes of determining the cost of LRIT for LRIT listeners and hence a criteria for selecting an LRIT architecture, current estimates suggest the cost of very basic LRIT position reports would be on the order of $0.10 per position fix per ship. This price will vary depending on any additional features the end-user may contract for and on the difficulty in obtaining these measurements by the TSP. However, such a number may be used to benchmark various architectures, e.g., for 65000 ships x 365 days/year x 1 data/hr x 24 hrs/day x $0.10/data = $57M/year might be a worst case figure for a system with no other overhead costs like DSSA. However, if sufficient overhead is added to LRIT information costs to bring it to, say $1.00 per position fix, cost for LRIT services could approach a ridiculous **$570M/year**.

---

[1] 65000 ships x 1000bytes/LRIT data x 8bits/byte x 1 LRIT data/hour/ship x 1/3600 hours/second x 200 LRIT listeners = 28Mbps

[2] Inexpensive off the shelf security solutions such as VPNs can be used by TSPs to distribute their delivery systems to take advantage of reliable, low cost bandwidth remotely. This would serve countries where connectivity is inaccessible or expensive.

[3] Often called “data fusion”

[4] By offering the source code to our prototype implementation at no cost, we hope to further remove barriers to implementation.

The Trade Off
In order to operate in a DSSA, a TSP should have reasonable Internet connectivity already by virtue of its need to service existing customers and to encourage new business and services. In a DSSA, the TSP must send LRIT information to every entity authorized to receive it. This shifts the burden from the CDB to the TSP, but reduces the overall burden by a factor equal to the number of TSPs. Where one copy of the information was sent from the TSP to the CDB for redistribution, now it must send 100's of copies directly to the entitled entities. However, since each TSP is only responsible for its limited number of vessels, the required bandwidth is greatly reduced relative to the CDBA and usually supported by the TSP's existing connection. Difficulties in obtaining even this bandwidth for some TSP's can be addressed by various remote hosting techniques as described previously. Using the same calculation as before and assuming a small number of TSPs (including national vessel monitoring systems, fleet management systems, and other vessel reporting systems), say 14, suggests a 2Mbps (E1) connection would be sufficient for a TSP to support even peak requirements[5]. TSP's we have consulted with do not see this requirement as a difficulty. Regardless of implementation it should be noted that the total Internet bandwidth consumed by a DSSA is the same as that of the CDBA since the CDBA also requires the transmission of LRIT info from all TSP's to all authorized entities. We feel this is a minor tradeoff for achieving the greater end-to-end security, reliability, scalability to any number of vessels, fast deployment, and pro-competitive pro-innovation environment that a DSSA provides.

A Distributed Secure Scalable Architecture (DSSA) for LRIT

The features of a Distributed Secure Scalable Architecture include end-to-end security, fault tolerance, low cost by obtaining LRIT information directly from TSPs, and distributed bandwidth and grid computing to handle any number of vessels. The DSSA benefits from the continuing investment and improvements to the Internet infrastructure and scales to handle multiple tracking service providers without reconfiguration. Secured access and identity management are conducted via proven Public Key Infrastructure methods in concert with a certificate revoke list. A common open standard extensible interface specification for TSP encourages the entry of more participants, greater competition and lower cost. DSSA is an open system that does not preclude other architectures (including centralized) and may simultaneously support them. Filtering and control of each nation's flag ships is controlled by that nation through direct contact with the TSP, usually in that country, further distributing oversight responsibilities. The DSSA can be deployed quickly since it is based on existing infrastructure and open standards. There are little or no start up costs using existing infrastructure. Competitive: Driven by commercial and customer interests. Conducive to innovation and new developments. Contractual simplification

How it works (refer to Fig 1 and Fig 2)[6]
What follows are the steps taken by TSP and LRIT listener when they first come up.

1. When a LRIT listener first comes up it looks up the connection information for each TSP using the Internet Domain Name System (DNS).

[5] For a bandwidth challenged TSP, off loading the redistribution function to a well connected site would reduce the bandwidth requirements of the TSP to sub-64kbps. Note however, for the case where the TSP and entity receiving LRIT information are housed in the same facility that approximately 140kbps would be required to receive such data.
[6] As it develops a prototype complete with free source code will be available at http://lrit.xtcn.com

2. For each TSP, the LRIT listener performs an initial public key security handshake that certifies the identity of each end of the connection and assigns randomly generated bulk encryption keys[7]. Even if there were 1000's of TSPs to contact, this represents an insignificant number compared to the traffic a typical server experiences on the Internet.
3. The connections now remain idle until the TSP has LRIT information to send. LRIT information is sent[8] subject to calculations and data (e.g. contour maps, sail plan) based on the identity of the LRIT listener, i.e., Flag state, Coastal state distance and the flag state Administration has not requested blocking, or Port state (based on a sail plan filed by the ship owner)
4. On occasion (equipment replacement, link failure, power outage, updates, new TSPs etc) the TSP or LRIT listener will perform a new security handshake to update keys and re-establish identities. Since the handshake happens quickly, no data is lost.
5. Also on occasion, the IMO Certificate Revocation List (CRL) will be checked by LRIT listener and TSP to determine if there are any participants whose certificates should not be trusted.
6. Once identities and security have been established, a LRIT listener may, instead of passively receiving information, request information on specific ships and receive this information if authorized and agreed with a TSP.
7. The flexibility of a DSSA does not restrict governments from creating their own central databases alone or with others to address their needs.

Billing/Charging

Potential LRIT TSPs have indicated that there would be no difficulty with respect to billing. Companies understand billing issues and are inherently motivated to streamline the process for their customers (e.g., using credit cards, automated EFT payments or through clearing houses). A Contracting Government would only need a credit card or other accounting information, just as would be used to complete any on-line transaction. A DSSA does not preclude the use of facilitating agencies, existing or new, to handle billing, if so desired by states, TSPs or both.

Oversight

A distributed LRIT architecture benefits from the natural oversight that is a direct result of market forces and competition. TSP's will be driven by customers needs which ensures the proper functioning and servicing of these needs whether they be technical, administrative or even political[9]. Therefore, we must ask what we want from oversight, particularly in a distributed architecture, and clearly define it before imposing any regulations that may stunt a potentially vibrant market.

IMO still holds ultimate control over all the players in LRIT because IMO holds the root certificate (and its corresponding private key) which must be used to renew the certificates used

[7] The physical security and management issues of having shared/common keys is completely avoided by using this public key approach which is based on existing standards such as SSL and TLS. Identities are guaranteed and strong (AES) encryption maintained. Note: Authentication may be initiated by either side as may be the case for a temporary or mobile LRIT listener. PKI in short uses a pair of very long keys, a private and public key. One is used to decrypt data encrypted by the other.

[8] The LRIT listener may reject information on a particular vessel in favor of a lower cost alternative provider should duplicate sources exist or if the listener does need information on this vessel and not want to pay for it. Other mechanisms could be supported as well.

[9] Since the businesses' relationships between the non-intergovernmental, national, often commercial TSPs are out of the scope of IMO regulation, no LRIT architecture or approach can keep LRIT information from being sold directly (via contract or bilateral agreement) to end-users so long as it does not violate the sovereign laws of the nations involved.

by everyone as they expire[10]. It also controls the certificate revocation list, placement on which would disable participating in the LRIT system by revoking a bad player's certificate. This amounts to essentially a digital contract. Finally, since IMO also controls the LRIT DNS SVR entries for TSPs (and possibly LRIT listeners)[11], it may remove such entries to disable a bad player in short order as well.

In a DSSA LRIT, Contracting Governments would already have a relationship with the TSP(s) they use to track their vessels to ensure, 1) that they abide by there wish to limit access to certain states for LRIT information, 2) that they properly handle sail plans (port state information), and 3) maintain an acceptable cost-benefit for services. With this watchful eye over the entity controlling information on their ships (which might be within their national borders and therefore subject to closer supervision), it makes sense for this same Contracting Government to perform this component of oversight. In effect, this customer-business relationship directs a natural, robust, and free oversight with respect to ensuring the integrity and adherence to the functional specifications of the LRIT system (if I don't get what I want, you wont be able to sell information on my ships).

Finally, a DSSA for LRIT may serve to streamline some of the remaining oversight functions by automating auditing and reporting functions by providing special access codes and report generation (possibly sanitized) software[12] to verify and statistically analyze the behavior of the TSPs. This would hopefully lead to greatly reduced oversight costs and better service for states.

Implementation

In a DSSA, there is no requirement for initial funding by states. A common interface specification between LRIT listeners and Contracting Governments is all that is needed.. Initial certificate signings by IMO can be done at the next IMO meeting when delegates and TSPs are present as official representatives of their respective countries and companies. They will need to have their electronically generated certificate request (which may be done on an embassy computer) and connection information (domain name) for their LRIT listener(s). After the certificates are e-mailed back and applied to their LRIT listeners, their system is ready to start receiving LRIT information and will do so as TSPs also apply their IMO signed certificates.

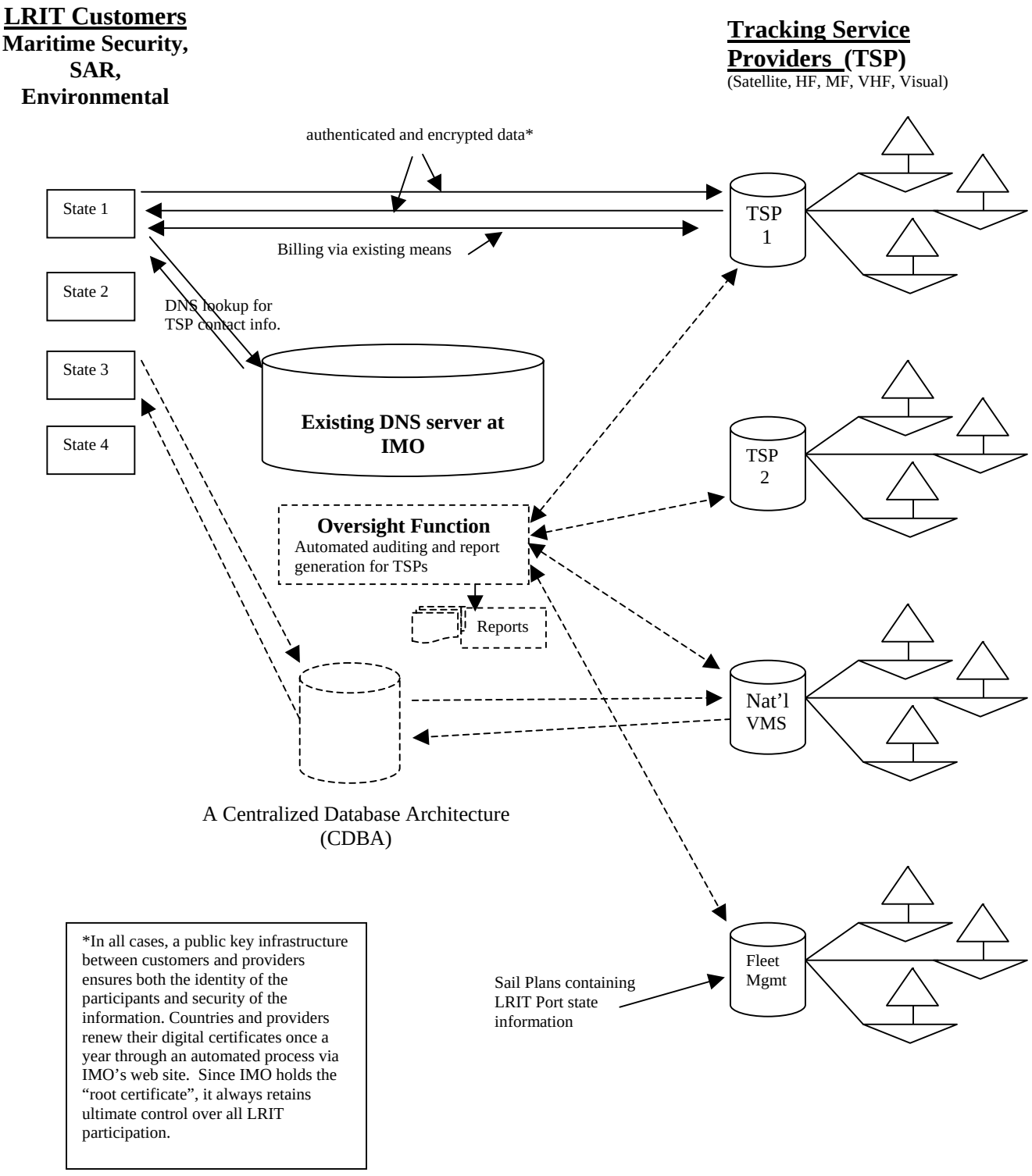
---

[10] Although completely at the discretion of IMO, 12 months is common lifetime for SSL and other PKI certificates and might be a good default for TSP and LRIT listener certificates as well from the viewpoint of security.

[11] One or two line entries in a file read by IMO's DNS server. Every organization has a DNS server.

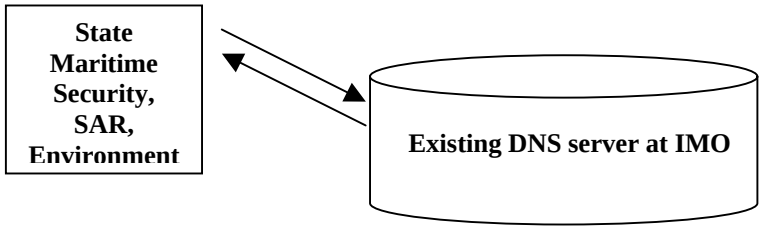
[12] The system described here would provide automated report generation that would allow states, the Committee or sub-committee, or an oversight organization to assess TSP adherence to regulations, performance, etc. Since the report generation process would be automated, reports may be generated frequently and made available via the IMO Web site. All of these conditions lead to a more flexible, effective, lower cost system.

Fig 1 - A Distributed Secure Scalable Architecture (DSSA) for LRIT

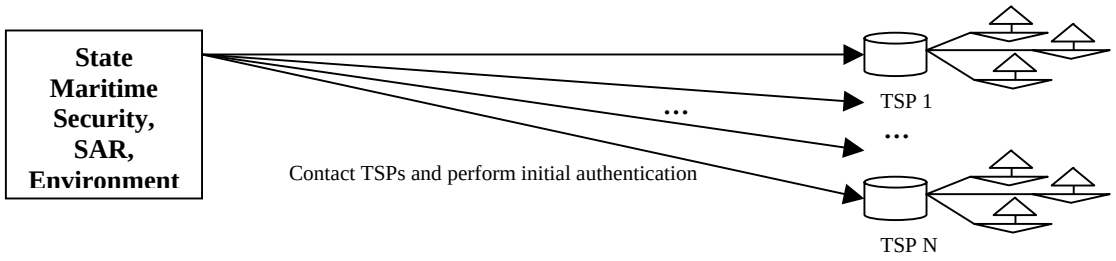


Richard Lamb lambrh@state.gov

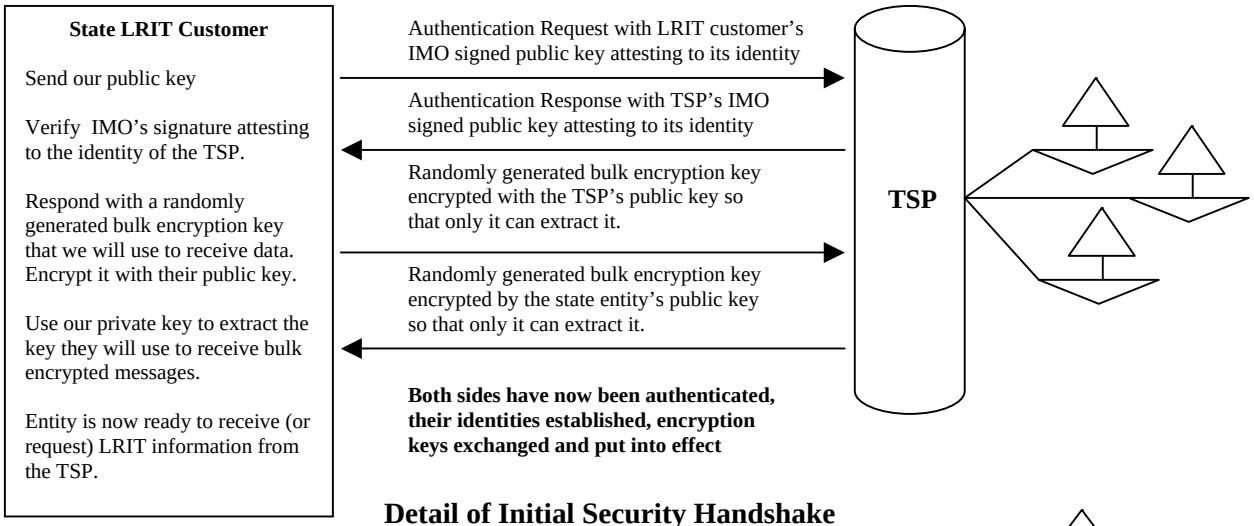
Fig 2 - Steps in a Distributed Secured Scalable Architecture Protocol



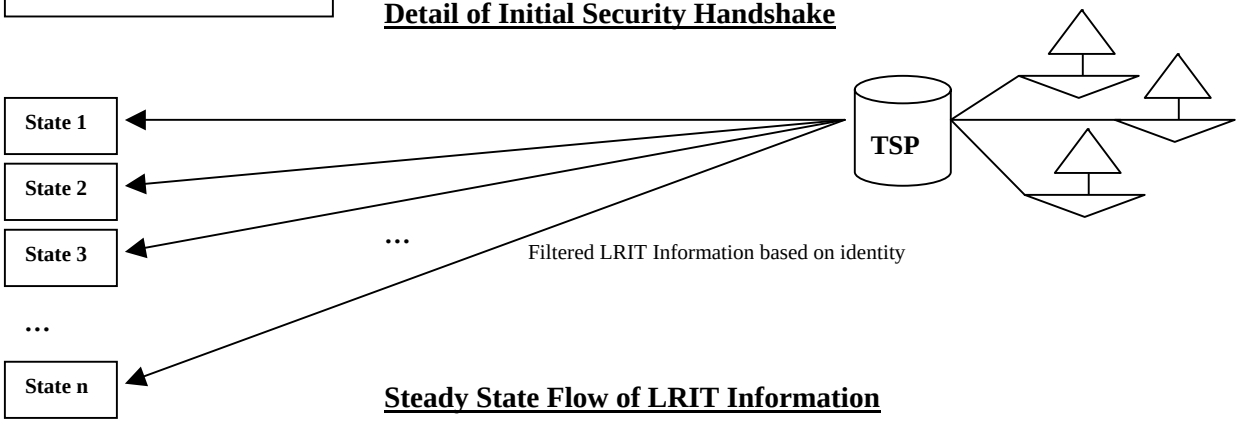
Lookup Internet information for TSPs at power -up



Initial Security Handshakes



Detail of Initial Security Handshake



Steady State Flow of LRIT Information

Richard Lamb lambrh@state.gov