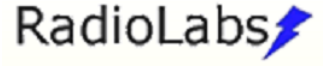
# Locksat

## LOCal Key Synchronization and generation for data security in sATellite communications

| ITI Type A activity: Proof of Concept | | |
|---|---|---|
| Inventor | PXL |  |
| Inventor | Radiolabs |  |

## Introduction

LOCKSAT is the acronym of LOCal Key Synchronization and generation for data security in sATellite communications.

Locksat can be regarded as a security key renewal algorithm that allows frequent key renewal (re-keying) without exchanging data messages over un-secure channels.

In order to guarantee high degree of security for data exchanged in a communication channel, secure cryptographic transforms and efficient key management systems must be implemented.

Keys and cryptographic transforms may protect exchanged data from tampering, eavesdropping and other security threats. Frequent re-keying is one of the key issues in order to guarantee a high degree of security.

In satellite environment propagation delay strongly impact re-keying performance because each re-keying phase requires at least one or two round-trip time.

Being the key distribution performed via satellite, the cost of the operation can

be high because the bandwidth is expensive and the delay is meaningful.

## The Innovation

In order to mitigate the aforementioned problems, Locksat propose an innovative key management system allowing the independent local key generation and synchronization at both ends of the communication link. Generated keys are used by data streams to protect traffic. Communication parties agree on an ordered set of keys that changes on a time basis.

Locksat approach has a number of advantages: it allows frequent re-keying avoiding long round trips typical of satellite links, it reduces bandwidth consumption for signaling purposes and simplifies re-keying procedures for multicast groups.

This solution is innovative since all the current standard solutions (e.g. IKE, DVB-CA, etc.) are based on key exchanges over the channel, that could be detrimental over satellite links.

Locksat concept can be used to supply key management for security services implemented at various layers of the OSI stack (e.g. IP layer, Application Layer, Link layer etc.) for various configuration scenarios.

The concept of Locksat is derived from similar concepts already successfully applied to other fields like spread spectrum frequency hopping systems. Those systems use a similar concept for the synchronization of frequency hops between transmitter and receiver. In that case local generation and synchronization of frequency indexes is realized by communication parties in order to timely program the hopping sequences without exchanging data. This concept is replaced in Locksat with the generation and synchronization of security keys for all the communication parties.

## Results of the ITI Activity

The ITI project activity included the concept validation with the demonstration of Locksat applicability to satellite applications and the definition of its advantages compared with existing key management techniques.

This task has been accomplished with the following work phases:

- Definition of general idea of Locksat. Locksat algorithm has been designed to work at different level of protocol stack and for different application scenarios.
- Selection of satellite application scenarios on the basis of three main criteria: diffusion, market penetration of applications and integration in standard architecture/protocols. This activity led to the selection of two scenarios: TV-Broadcasting and IP data over satellite.
- Adaptation of Locksat concepts to aspects related to the selected scenarios including integration in standard architecture/protocols. Two design were produced; a DVB-CA compliant design for TV-Broadcasting and an IPsec integrated design for VPN endpoints in a DVB-RCS-IP network.
- Design and implementation of simulation tools to validate the Locksat idea in the satellite environments.
- Simulation runs and result analysis to collect performance statistics for validating Locksat effectiveness and comparing it with other solutions.
- Preliminary definition of Locksat implementation implications for the two scenarios in order to asses future work.

Summarizing the results achieved for the two selected application scenarios, for DVB-RCS-IP scenario:

- The Locksat concept and its adaptation has been successfully proved through simulations.
- In high stress condition (network always congested and high delay variations) Locksat grants good performance compared to IKE/IPsec (key lifetime of 2,5 sec).
- In normal condition Locksat supports key lifetime < 0,5 sec (less than physical RTT delay).
- No data is exchanged to renew keys, while IPsec/IKE for AH service needs a bandwidth of 3.4-5.1 kbit/sec to achieve its theoretical limit (key lifetime of 3-4 sec). This value increases when other security services are used at the same time.
- Stress points for Locksat at IP level have been located in large communication channel delay variations.
- Mitigation for these stress point have been also provided .

While for DVB-CA scenario:

- The Locksat concept and its adaptation has been successfully proved through analysis of real traffic traces.

- Locksat improves the performance of the current CA implementations allowing a key renewal time of approximately 25 msec compared to the current 10 sec.
- No data is exchanged to renew keys, while current CA algorithms uses ECM messages for an average bandwidth of 150 kbit/sec for 10 channels in a transponder.

## Future Applications

Locksat can be applied to the two mentioned satellite application scenario used to validate the concept:

- Conditional Access in Satellite TV Broadcasting.
- IP data services over satellite links.

Apart from the two already mentioned application scenarios some other satellite applications were envisaged during the project final meeting:

- Secure satellite control and telemetry links.
- Secure links used to download earth observation data.

Summarizing Locksat key management scheme may be applied at different levels of the OSI protocol stack (eventually tailoring to specific protocol characteristics) and may be successfully applied:

- In links with large RTT.
- When frequent key renewal is required.
- When key renewal must occur without exchanging data (for security issues).
- When bandwidth is a precious resource and security is needed.
- When large data transfers must be performed without interruptions due to security key exchanges.
- In links with limited delay variations allowing very high key renewal frequencies.

## Contacts

| | | |
|---|---|---|
| | Contractual Manager | Mr. Giovanni Pico<br>g.pico@pxl.it<br>www.pxl.it<br>tel. +39 06 44.23.25.20<br>fax. +39 06 44.26.29.08 Via Re Tancredi 8, 00162, Roma, Italia |