The SaNTA Project

André Rosado
Skysoft Portugal, S.A.
arosado@skysoft.pt

José Brázio
Instituto de Telecomunicações/Inst. Superior Técnico, Lisbon Tech. University
jose.brazio@lx.it.pt

ESTEC, December 2, 2008
## Overview

- **Introduction**
  - Project partners, history, problem areas, phases
- **Phase 1**– TPRMMSN
- **Phase 2**– SaNTA
- **Phase 3**– SaNTA security
- **Comparison with PEP architecture**
- **Phase 4**– DVB-RCS trials
- **SaNTA Usage Cases**
- **Concluding Remarks**
<table>
<thead>
<tr>
<th><strong>Project Partners</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ ESA was the main stakeholder of the SaNTA project</td>
</tr>
<tr>
<td>▪ Skysoft was the Prime Contractor of the SaNTA project</td>
</tr>
<tr>
<td>▪ IT was the Subcontractor of the SaNTA project</td>
</tr>
</tbody>
</table>
Partners – Skysoft Portugal

Leading Portuguese Supplier of the European Space Agency (ESA)
Leading Portuguese Company in Software Engineering for Civil Aviation
Reference Portuguese Company for European Commission (EC)

- Software & Systems Engineering Company
- Founded in 1998
- Based in Lisboa
- Turnover expected 2008: ≈ 6.5 M€
- Human Resources: ≈ 90 Eng.
Partners – Skysoft Portugal

OPERATIONAL AREAS

A) Aeronautics, Aerospace, Security & Defence:
- Safety Critical Software
- Integrated Modular Avionics
- Integrated Security Systems
- Air Traffic Management System
- Defence Data Networks & Systems
- Satellite Navigation
- Ground Segment (PDS, SCC)
- Satellite Communications Systems
- Link 11 / Link 16 Data Translator
- Maritime Surveillance
  - AIS, VTS, SAR Integration

B) Telematics & Business Solutions:
- Intelligent Transport Systems
- Mobility (LBS, GIS, FM)
- IT & Business Solutions

• Outstanding System & Software Engineering
• R&D Partnerships
• Institutional Space & Defence Markets
• Strong Customer Focus
• Engineering Solutions and Applications

Technologies Mastering

SatCom Avionics
Navigation Maritime

Key Contribution Infrastructure & Institutional Programmes

Market Applications

GALILEO
GMES
PASR
...

Aero-Space & Defence

Mobility
Security
Intelligent Transport Systems
Surveillance
Partners – IT

• Instituto de Telecomunicações (IT)
  • Private, not-for-profit organization, association of
    – Instituto Superior Técnico, Lisbon Technical Univ.
    – University of Aveiro
    – Faculty of Sciences and Technology, Univ. of Coimbra
    – Portugal Telecom Innovation
    – Nokia-Siemens Networks
  • Includes about 180 PhD researchers
  • Covers areas ranging from material sciences, microwave, electronics, and circuit design, to networking and multimedia communications
### SaNTA Project—History

**ITT**
- issued on the 29th of March 2000, from the Department of Communication Satellites of ESTEC, in the scope of ASTE program (ref. MS 1.2), ARTES 5 budget
- ESA Technical Officer: Mr Erling Kristiansen
- Contemplated two phases

**Objectives**
- develop a transport architecture and protocol to replace TCP, optimised for the mobile satellite network environment
- implement measures to maximise the efficient utilization of satellite networks by providing improved ways to manage resources

**Consortium**
- Skysoft (prime) + Instituto de Telecomunicações (IT) (sub-contractor)

**Contract**
- Awarded on 19th of June 2001, in parallel with two other consortia
Problem Areas

- Efficient end-to-end transport service
  - Mitigation of TCP end-to-end performance degradation under
    - high loss rate
    - large propagation delay
    - asymmetric forward and return channel bandwidths

- Resource management
  - Dynamic assignment of satellite link resources in accordance with varying traffic demands
    - Model: availability of mechanisms for capacity allocation/deallocation via explicit signaling
## Project Phases

- **Phase 1**
  - definition of the transport architecture and protocols and of the resource management concept; basic validation
    - ended March 2003

- **Phase 2**
  - prototype implementation and test in lab environment
    - ended November 2004

- **Phase 3**
  - introduction of security features; prototype enhancement and validation
    - ended November 2005

- **Phase 4**
  - test in DVB-RCS environment (AmerHis)
    - started March 2007, ended February/2008
SaNTA Project

- SaNTA Technological Development

TPRMMSN

- Proof of Concept
- Protocols and Architecture Design

SANTA (Phase 2)

- Test-Bed
- Protocols and Architecture Implementation
- Lab Trials

SANTA Sec (Phase 3)

- Introduction of Security Features
- Prototype Enhancement and Validation

SANTA AmerHis (Phase 4)

- Testing in DVB-RCS environment

Timeline:
- Jun 2001
- Mar 2003
- Aug 2003
- Nov 2004
- Nov 2005
- Mar 2007
- Feb 2008
Phase 1–TPRMMSN

• Study phase, leading to
  – A transport architecture providing
    • efficient end-to-end transport service across heterogeneous network segments
    • flow control between terrestrial and satellite links across resource management and interworking units
    • ability to offer different types of services to applications, depending on communication requirements, through a resource management policy
    • end-to-end semantics
  – A transport protocol suitable for satellite links
  – A resource management concept
    • encompassing the interaction with applications and satellite resource management network entities
Transport Architecture Approach

- Conceptual network and service model
  - end-to-end path seen as sequence of homogeneous transport network segments (TNS)
  - use within each TNS of a reliable flow-controlled connection-oriented transport protocol, adapted to that TNS
    - TCP in terrestrial segments
    - *ad-hoc* protocol over satellite link
  - new upper layer located at user terminals and at network elements joining adjacent TNSs (InterWorking Unit, IWU) [cf. Sec. 12.4.1 of ETSI TR 101 985]
    - between TNSs, relays data between their associated transport protocols (almost like an application)
    - at user end systems, passes data between applications and local transport service
  - end-to-end flow control via backpressure
Transport Architecture

[Diagram showing transport architecture with different components and connections, including End User A, End User B, IWU A, IWU B, WAN A, WAN B, Satellite dish, Application, TVC 1, TVC 2, TVC 3, TNS 1, TNS 2, TNS 3, ITL, TCP/UDP, IP, L2 LAN, L2 SAT, L2 WAN, SaSTP.]
## Pros/Cons

**Advantages**
- Split architecture
  - gives consistently better performance, with the right satellite transport protocol

**Disadvantages**
- Breaks end-to-end semantics of TCP
  - no big deal, but new layer keeps end-to-end semantics anyway
- Needs keeping state
  - Not a technological problem
- Needs changes to user communications stack
  - (more on this later)
- Classical split architectures do not allow use of network-level security (IPSec)
  - (more on this later)
Resource Management Approach

- Make resource management functions available to applications and interworking units, in order to manage satellite resources on the basis of traffic information.
  - Resource Management (RM) entity in IWUs collects local measurements and information obtained from RM-enabled user terminals for requesting from an NCC bandwidth manager the allocation/deallocation of satellite link bandwidth.
**Design Requirements**

- **Architecture**
  - Support of end-to-end data transfer allowing high satellite link utilization
  - Capability to ensure routing of traffic through specific satellite gateways
  - Capability to fall back into standard TCP operation
  - Support of specific network configurations

- **Communication services**
  - End-to-end unicast reliable connection-oriented (RCO) service, with flow control functions [elastic traffic]
  - End-to-end unicast unreliable connection-oriented (UCO) service [stream traffic]
  - End-to-end unicast unreliable connectionless (UCL) service
Design Requirements

• Interface to applications
  – Compliant with standard TCP/UDP interface

• Resource Management (RM) functions
  – Provision of mechanisms for the exchange of RM information between applications, Resource Managers at IWUs, and NCC bandwidth managers
ITL Protocols

- ITL protocols defined for connection-oriented and connectionless services
  - Connection-oriented service protocol was specified covering
    - Connection management (set-up, release, failure)
  - Idle connection handling
  - Data transfer
  - Resource management information transfer
- Connectionless service
  - Data transfer
  - Resource management information transfer
Satellite Link Transport Protocol

- Transport protocol over satellite link is required for reliable services
  - Functionality included
    - Connection set-up and tear-down
    - Reliable transfer of user data
    - Flow control
  - Functionality *not* included
    - Congestion control
    - Reordering/resequencing of packets
  - Protocol was designed based on LAPB, with modifications on
    - flow control: employ an advertised receiver window (*à la* TCP)
    - support for dual IP addresses (for network elements in asymmetric configurations)
    - support for multiple instances of execution
## Design, Validation, Verification

- Implementation Design supported on SDL specification via automated tool
- Separate validation activities for
  - Satellite link transport protocol
  - End-to-end architecture
- Correctness validation
  - Coverage/reachability analysis, livelihood properties
Performance Assessment

- Preliminary performance assessment
  - Specific focus on data transfer issues
  - Via simulation and emulation
    - ns2 simulator for TCP end-to-end assessment and satellite transport protocol
    - In-house emulator for new architecture, allowing insertion of real network segments

- Items of interest
  - Maximum throughput/satellite link utilization (heavy traffic conditions)
  - Packet transfer delay
  - System stability / buffer behavior with respect to packet losses (random errors or link outages) or capacity changes

- Overall satisfactory results
Phase 2 – SaNTA

- Objectives
  - Re-establish requirements from Phase 1
  - Re-define architecture and design from Phase 1
  - Perform a pilot implementation of the protocols
  - Perform a demonstration and performance measurement in a realistic environment
    - The demonstration environment may partly rely on simulation of components that are difficult or too costly to access.
Redesign

- Design developed in Phase 1 was interesting, but...
  - ... people don’t want to change their terminal software
    - Unreliable connection-oriented service is out
    - Use of a modified protocol stack is out, including Resource Management (RM), at least in fixed terminals
  - ... DVB-RCS systems are on the way
    - Asymmetric configuration is out
  - Think of a solution where changes are made to network elements at the point of interconnection to the Internet (routers, firewalls)
    - Modified protocol stack can be left in mobile terminals; RM can be left in these and in IWUs
  - Solution based on proxy ideas? Yes!
A Proxy-Based Solution

- Delegate ITL functions out of fixed user terminals
  - Functionality of new protocol layer, formerly at user terminal, is migrated to “Satellite Enhancer” (SE) network element
    - Replaces Internet access router
    - Acts as a proxy: detects requests for new TCP connections and replies to these requests and sets up corresponding ITL connections; same for connection termination
Split architecture operation

End User A

Application

IP

L2 LAN

TVC1

ITL

TCP/UDP

IP LAN

L2 LAN

SE A

WAN A

TNS1

TVC2

ITL

TCP/UDP

IP LAN

L2 LAN

Satellite dish

TVC3

ITL

TCP/UDP

IP LAN

L2 LAN

SE B

WAN B

TNS3

TNS2

End User B

Application

TCP/UDP

IP

L2 LAN

Satellite dish

SaSTP

WAN A

IWU A

TVC

1

SE A

WAN A

ITL

TCP/UDP

IP LAN

L2 LAN

SaSTP

WAN B

IWU B

TVC

3

SE B

WAN B

ITL

TCP/UDP

IP LAN

L2 LAN

SaSTP

TNS

2

TNS

1

TNS

3
Connection Set-up

Terminal A -> SE A -> IMUA -> MUB -> SE B -> Terminal B

1. appA connect (IP_B, port_B)
   - TCP: listens up TCP

2. SYN (DEST=IP_B)
   - TCP: waits for SYN

3. SYN+ACK (SRC=IP_B)
   - TCP: sends SYN+ACK

4. ACK (DEST=IP_B)
   - TCP: waits for ACK

5. SYN (SRC=IP_A)
   - TCP: waits for SYN

6. ACK (SRC=IP_A)
   - TCP: waits for ACK

7. CC ()
   - TCP: waits for CC

8. ACK (DEST=IP_A)
   - TCP: waits for ACK
Data Transfer

App. A:
- send (IP_B, port_B)

IP* looks up ITL-Aware routing table
- If IP_B is a local IP:
  - IP* passes TCP segment to TCP
  - TCP: returns ACK to A
  - ITL: receives ACK, extracts data
  - ITL: determines next hop (IWU_A)
  - ITL: formats DATA
  - ITL: sends DATA through TCP connection to IWU_A

ITL: changes DATA (VCI switching)
- ITL sends DATA to IP_IWU_B via SaSTP connection

ITL: extracts data
- ITL: sends ACK (SRC=IP_B) to SE_B
- ITL: sends DATA to IP_IWU_B via UDP

If IP_A is a local IP:
- IP* passes ACK to TCP
- TCP: returns ACK to A
- ITL: receives ACK, extracts data
- ITL: sends ACK (DEST=IP_A) to SE_B

App. A:
- sendto (IP_B, port_B)

IP* looks up ITL-Aware routing table
- If IP_B is a local IP:
  - IP* passes UDP segment to UDP
  - ITL: receives, extracts data
  - ITL: determines next hop (IWU_A)
  - ITL: formats DG
  - ITL: sends to IWU_A via UDP

ITL: changes DG
- ITL sends DG to IP_IWU_B via IP

If IP_A is a local IP:
- IP* passes ACK to TCP
- TCP: returns ACK to A
- ITL: receives ACK, extracts data
- ITL: sends ACK (DEST=IP_A) to SE_B
Network Elements

- Satellite Enhancer (SE)
- InterWorking Unit (IWU)
Network Elements

- Mobile Terminal
Performance Tests

• Lab Test Bed
Test Results

- Steady State Throughput (Satellite Link Utilization)
  256 kbit/s, 1 connection

![Graph showing steady state throughput for different BER and PER values with SaNTA Architecture and End2End TCP, and maximum theoretical throughput.](graph.png)
Test Results

- Steady State Throughput (Satellite Link Utilization)
  - 256 kbit/s, 2 connections

![Graph showing test results]

- BER=0
- BER=1E-6, PER≈1.1%
- BER=5E-6, PER≈5.5%
- BER=1E-5, PER≈10.8%
- BER=2E-5, PER≈20.4%

- SaNTA Architecture, ITL Buffer Size = 2
- SaNTA Architecture, ITL Buffer Size = 5
- SaNTA Architecture, ITL Buffer Size = 20
- End2End TCP
Test Results

- Steady State Throughput (Satellite Link Utilization)
  - 256 kbit/s, 5 connections

![Graph showing Steady State Throughput with different BER values and ITL Buffer Sizes]
Test Results

- Steady State Throughput (Satellite Link Utilization)
  - 256 kbit/s, 10 connections

Graph showing Steady State Throughput with varying BER and error rates.
Test Results

Steady State Throughput (Satellite Link Utilization)
Asymmetric links, 1 connection, SaNTA

- BER=0
- BER=5E-6, PER=5.5%
- BER=2E-5, PER=20.4%

KBytes/s

- 1Mbit/s: 128Kbit/s
- 1Mbit/s: 64Kbit/s
- 1Mbit/s: 32Kbit/s
Test Results

- Steady State Throughput (Satellite Link Utilization)
  Asymmetric links, 1 connection, TCP
Test Results

- Bandwidth Sharing, Steady State
  No bit errors, ITL Buffer Size = 5
Test Results

- Satellite Link Outage
  No bit errors
Test Results

- Satellite Link Outage
  BER = 5e-6
Test Results

- Dynamic Fairness
  - No bit errors
## Phase 3 – SaNTA Sec

- **Objective**
  - Develop a Security Architecture for SaNTA
- **Work led by A. Zuquete, University of Aveiro**
  - Only main points referred here
  - Details available in
<table>
<thead>
<tr>
<th>Phase 3 – SaNTA Sec</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>• SaNTA security-related issues</strong></td>
</tr>
<tr>
<td><code>- End-to-end confidentiality</code></td>
</tr>
<tr>
<td>• Prevents SaNTA from accessing transport headers</td>
</tr>
<tr>
<td>• Example: layer-2 VPNs (PPTP, L2TP), IPSec confidentiality</td>
</tr>
<tr>
<td><code>- End-to-end peer authentication</code></td>
</tr>
<tr>
<td>• Prevents SaNTA from impersonating end hosts/networks</td>
</tr>
<tr>
<td>• Example: IPSec authentication of origin/destination hosts</td>
</tr>
<tr>
<td><strong>• Activity goals</strong></td>
</tr>
<tr>
<td><code>- Intrinsic security</code></td>
</tr>
<tr>
<td><code>- Security tolerance</code></td>
</tr>
<tr>
<td><code>- Architectural solution</code></td>
</tr>
</tbody>
</table>
## Topological Deployment

**SEs**
- Should belong to the infrastructure of SaNTA clients
  - Within an isolated DMZ
  - On network gateways
- Should be completely or as much as possible managed by clients
  - End-networks administrators choose the right approach to route authorized traffic into SaNTA through a local SE
  - Should be protected from inside or outside attacks
    - To prevent usage abuses of satellite links imputable to SEs' owners

**IWUs**
- Deployed and managed by satellite link providers
- Behave as Internet routers with SaNTA capabilities only for authorized SEs
**Trust and Access Control**

- **SaNTA must be trusted by end-nodes/networks**
  - Contractual relationship between the end-nodes and the company selling the services of a particular SaNTA infrastructure

- **Correct exploitation**
  - It should be used only by authorized end-users or by authorized end-nodes/networks
  - It should not be abused by any Internet nodes

- **Elementary authorization policy**
  - SEs should only communicate with authorized peers
  - IWUs should only communicate with authorized peers

- **Mechanisms for enforcing the authorization policy in SEs and IWUs**
  - Packet-filtering firewall for dropping unintended traffic
  - Strong authentication mechanism for authenticating IP peers
### Security Service Goals

- **Transparency**
  - No security mechanisms directly provided to end-nodes and applications
    - SaNTA should be similar to an Internet core router
  - No interference with security requirements of end-nodes and applications

- **Secure added value**
  - Protect all SaNTA traffic
  - Do not introduce new vulnerabilities in the traffic accelerated/tunneled

**Issues**
- Peer Authentication
- Protection of the data flows
- Availability
Security Services

- Peer Authentication

Mutually authenticated access

Possible authenticated access

Pretended end-to-end interaction

ITL Virtual Circuit / Tunnel
Security Services

• Protection of Data Flows
Proposed Security Technologies

Secure TCP data flows
Proposed Security Technologies

Secure UDP data flows

Pretended UDP interaction

ITL UDP tunneling

IPSec AH

IPSec ESP confidentiality and authentication

UDP Datagrams

N1

SE1

IWU1

IP header (SE1-IWU1)

AH header SA SE1-IWU1

UDP header

UDP payload

ITL header (using UDP/IP address from N1 & N2)

UDP original payload (encrypted, ESP SE1-SE2)

N2

SE2

IWU2

IP header (IWU2-SE2)

AH header SA IWU2-SE2

UDP header

UDP payload
Proposed Security Technologies

Secure “Opaque” data flows

<table>
<thead>
<tr>
<th>N1</th>
<th>SE1</th>
<th>IWU1</th>
<th>IWU2</th>
<th>SE2</th>
<th>N2</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP header (N1-N2)</td>
<td>IP header (SE1-IWU1)</td>
<td>IP header (IWU1-IWU2)</td>
<td>IP header (IWU2-SE2)</td>
<td>IP header (N1-N2)</td>
<td></td>
</tr>
<tr>
<td>AH header SA SE1-IWU1</td>
<td>AH header SA IWU1-IWU2</td>
<td>AH header SA IWU2-SE2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP header</td>
<td>UDP header</td>
<td>UDP header</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any payload</td>
<td>ITL header (using UDP/IP address from SE1 &amp; SE2)</td>
<td>Original payload encapsulated in SE21-SE2 datagram (encrypted, ESP SE1-SE2)</td>
<td>Any payload</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Proposed Key Management

- **Authentication keys**
  - Two possibilities, first is preferable
    - With asymmetric cryptography and X.509 certificates
    - With secret, symmetric pre-shared keys

- **Session keys**
  - Approach
    - Give clients all the relevant tuning options (inter-SEs policies are client-defined)
  - Inter-SEs Authentication
    - For SSL sessions protecting TCP payloads
    - Client-defined possibilities
  - Issues
    - Perfect Forward Secrecy (PFS)
    - Rekeying
SaNTA vs. PEP Architectures

- **Performance-wise**
  - Both are split architectures
  - Performance depends mostly on satellite link transport protocol

- **Functionality-wise**
  - Presence of tunnel all the way to end-user intranet allows further degrees of control and further functionality
    - e.g., security functions/VPN transparent to end users
# Phase 4 – SaNTA AmerHis

## Objective
- Extensively test SaNTA prototype in a DVB-RCS environment

## Motivation
- Assess performance with a consolidated standard in the segment
- Compare results against TCP implementation
Phase 4 – SaNTA AmerHis

- RCST and IWU machines were placed at Madrid due to regulatory issues (frequency band) in Portugal regarding AmerHis antennas.
## AmerHis System Features

- Multimedia payload embarked in a commercial communication satellite system
- Regenerative System
- Support of open standards DVB-RCS/DVB-S
- Meshed Topology
- Dynamic management of bandwidth – DAMA protocol, with capacity categories CRA and RBDC
Main results

- SaNTA proved to be a more efficient implementation under the following conditions:
  - Heavy Load Conditions
  - High BER value on Satellite link
  - Different AmerHis configurations, varying values of SDR and PDR
    - $SDR \equiv CRA$, $PDR - SDR \equiv RBDC$
- SaNTA has a considerably higher throughput than TCP
- Evidence of the fairness mechanism implemented in SaNTA
Phase 4 – SaNTA AmerHis

- Comparison against TCP for Heavy-load conditions (20 Mb evenly distributed)
  - Throughput achieved for SaNTA (Average Throughput ~ 300 Kbps)

![Graph showing comparison between SaNTA and TCP](image)

- Graph indicates average data transfer rate (Kbps) for different numbers of simultaneous connections (1, 2, 5) and comparison with TCP.
Phase 4 – SaNTA AmerHis

- Comparison against TCP with BER (=1.5*10e-6)

- SaNTA measures correspond to an average data rate three times faster than TCP
Phase 4 – SaNTA AmerHis

- Comparison between SaNTA and TCP for different BER values

![Graph showing comparison between End2End TCP and SaNTA for different BER values.](image-url)
Phase 4 – SaNTA AmerHis

- Comparison between SaNTA trials with modification of SDR parameter (SDR=0, 20 and 200 Kbps)
  - Similar behaviour (parallel graphs), with SaNTA response to smaller transfers being directly determined by SDR value
SaNTA Usage Cases

**DECISION Project**

- Deployment of satellite solutions in the context of European Civil Protection operations

- Skysoft contributed in Satellite IP communications with SaNTA framework for mobility (using INMARSAT BGAN terminals)

http://www.esa.int/esaCP/SEMZBAEIQCAF_index_0.html
### SaNTA Usage Cases

**FLYSAFE Project**

- FLYSAFE – Aeronautics project focused on flight safety, dealing with traffic and ground collision and adverse weather conditions

- Skysoft involved in Data Link Solution to On-board request of weather information from Ground Station (Meteorological Center), using SaNTA Framework
SaNTA Usage Cases

FLYSAFE Project

FLYSAFE Flight Tests Communications System Overview
Concluding Remarks

• The SaNTA project has provided a fertile environment for experimenting with split architectures and satellite transport protocols
  – Some of its assumptions have been superseded by developments in DVB-RCS
    • mainly concerning resource management, itself a hot topic
  – Assumptions concerning end-to-end transport service continue up-to-date
    – Design options made make it somewhat far from the ETSI PEP architecture, but differences are not intrinsic

• What we have today is still a prototype but, overall, it has proved a reliable operational platform
Thank you for your interest!
Annex
SaNTA Security

André Zúquete
avz@ua.pt
Instituto de Telecomunicações/Universidade de Aveiro

ESTEC, January 6, 2006
4.2 SaNTA Sec Architecture

Welcome
Project Introduction
Objectives and Relevance

4. Achievements

Coffee
Results Vs Objectives
Future Features
Discussion Period and Close-Out
End of Session
4.3.1 SaNTA Security Architecture: Why something new?

- Most paradigms used in secure communication protocols enforce end-to-end security policies
  - Preventing intermediate nodes to take an active role in the communication

**SaNTA security-related issues:**

- **End-to-end confidentiality**
  - Prevents SaNTA from accessing transport headers
  - Example: layer-2 VPNs (PPTP, L2TP), IPSec confidentiality

- **End-to-end peer authentication**
  - Prevents SaNTA from impersonating end hosts/networks
  - Example: IPSec authentication of origin/destination hosts
4.3.1 SaNTA Security Architecture: Goals

- **Intrinsic security**
  - Provide security solutions for protecting SaNTA infrastructures
  - Provide security solutions for protecting data flows handled by SaNTA entities

- **Security tolerance**
  - Provide the adequate mechanisms to tolerate end-to-end security mechanisms

- **Architectural solution**
  - Use state-of-art security mechanisms solutions for providing security
4.3.2 Topological deployment (1/2)

- **SEs**
  - Should belong to the infrastructure of SaNTA clients

<table>
<thead>
<tr>
<th>Welcome</th>
<th>Project Introduction</th>
<th>Objectives and Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Achievements</td>
<td>4.3 SaNTA Security Architecture</td>
<td></td>
</tr>
<tr>
<td>Coffee</td>
<td>Results Vs Objectives</td>
<td>Future Features Discussion Period and Close-Out End of Session</td>
</tr>
</tbody>
</table>

- Should be completely or as much as possible managed by clients
  - End-networks administrators choose the right approach to route authorized traffic into SaNTA through a local SE
  - Should be protected from inside or outside attacks
    - To prevent usage abuses of satellite links imputable to SEs’ owners

- Within an isolated DMZ
- On network gateways
4.3.2 Topological deployment (2/2)

- **IWUs**
  - Deployed and managed by satellite link providers
  - Behave as Internet routers with SaNTA capabilities only for authorized SEs
### 4.3.3 Trust and Access Control (1/2)

<table>
<thead>
<tr>
<th>Welcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Introduction</td>
</tr>
<tr>
<td>Objectives and Relevance</td>
</tr>
<tr>
<td><strong>4. Achievements</strong></td>
</tr>
<tr>
<td><strong>4.3 SaNTA Sec Architecture</strong></td>
</tr>
</tbody>
</table>

- **SaNTA must be trusted by end-nodes/networks**
  - Contractual relationship between the end-nodes and the company selling the services of a particular SaNTA infrastructure

- **Correct exploitation**
  - It should be used only by authorized end-users or by authorized end-nodes/networks.
  - It should not be abused by any Internet nodes
### 4.3.3 Trust and Access Control (2/2)

**Elementary authorization policy**
- SEs should only communicate with authorized peers
  - Authorized end-nodes and well-known IWUs

**IWUs should only communicate with authorized peers**
- Well-known/authorized SEs and IWU peers

**Mechanisms for enforcing the authorization policy in SEs and IWUs**
- Packet-filtering firewall for dropping unintended traffic
- Strong authentication mechanism for authenticating IP peers
  - Example: IPSec authentication (preferably with AH)
### 4.3.4 SaNTA security services: Goals

#### A - Transparency

- No security mechanisms directly provided to end-nodes and applications.
  - SaNTA should be similar to an Internet core router
- No interference with security requirements of end-nodes and applications

#### B - Secure added value

- Protect all SaNTA traffic
- Do not introduce new vulnerabilities in the traffic accelerated/tunneled
### 4.3.4 SaNTA security services:

#### A - Transparency

**Two complementary approaches:**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Mitigation</strong></td>
<td><strong>2. Security added value</strong></td>
</tr>
<tr>
<td>Handle properly problematic traffics</td>
<td>Deployment of internal security mechanisms</td>
</tr>
<tr>
<td>• Follow a best effort policy</td>
<td>• For providing a similar protection of data flows</td>
</tr>
<tr>
<td>• Example: tunneling and relaying</td>
<td>• Example: IPSec-like security along the SaNTA path</td>
</tr>
<tr>
<td></td>
<td>They allow end-users to securely abandon their end-to-end security mechanisms for benefiting from SaNTA acceleration</td>
</tr>
</tbody>
</table>
4.3.4 SaNTA security services: B - Secure added value

Secure added value:

1. Peer Authentication
2. Protection of the data flows
3. Availability
### 4.3.4 SaNTA security services: B - Secure added value

#### 1. Peer Authentication

- **End-hosts/networks ↔ SEs**
  - Managed solely by the administrators of end-networks
  - They all belong to the same security domain
  - Each SE should interact only with an authorized set of hosts within the end-network it belongs to

- **Between SaNTA entities**
  - Mutual authentication
4.3.4 SaNTA security services: B - Secure added value

Peer Authentication
### 4.3.4 SaNTA security services:

#### B - Secure added value

---

**2. Protection of data flows**

- **IPSec-like security along SaNTA path**
  - Wide end-to-end security policy for protecting transport payloads
    - Between SEs
  - Per hop security policy for protecting the negotiation of ITL connections between SaNTA entities

- **Protection of radio-broadcasted traffic**
  - Rely on the previous mechanisms
4.3.4 SaNTA security services: B - Secure added value

Protection of data flows
4.3.4 SaNTA security services:

B - Secure added value

### Welcome

**Project Introduction**

**Objectives and Relevance**

### 3. Availability

#### 4. Achievements

#### 4.3 SaNTA Sec Architecture

- **Protection from abuses**
  - Unauthorized access attempts
  - Denial-of-service attacks

**Coffee**

**Results Vs Objectives**

**Future Features**

**Discussion Period and Close-Out**

**End of Session**
<table>
<thead>
<tr>
<th>Secure Communication Technologies:</th>
</tr>
</thead>
</table>

- **A – SSL/TLS**
- **B – SSH**
- **C – IPSec**

### 4. Achievements

### 4.3 SaNTA Sec Architecture

- Coffee
- Results Vs Objectives
- Future Features
- Discussion Period and Close-Out
- End of Session
4.3.5 Secure Communication Technologies

A - SSL/TLS

- **Useful features for SaNTA:**
  - Confidentiality, authentication and integrity control to critical Information used by SaNTA in the negotiation of ITL connections / tunnels
  - Confidentiality, authentication and integrity control to original TCP payloads encapsulated in ITL and exchanged between SEs

- **Possible integrations**
  - First requires ITL to use SSL instead of TCP
    - TCP over ITL over SSL over TCP
  - Two options for the second:
    - TCP over SSL over ITL over TCP
    - TCP over ITL over SSL over TCP
  - ITL over SSL is preferable
    - But the ITL state machine must be updated!
4.3.5 Secure Communication Technologies

B - SSH

• Useful features for SaNTA:
  – Same as for SSL

• Possible integrations
  – TCP tunneled into a inter-SE SSH session over ITL
  – TCP over ITL over an SSH session tunnel

• Better or worse than SSL?
  – Worse: no key management, no library
4.3.5 Secure Communication Technologies

C - IPSec

• Useful features for SaNTA:
  – Source authentication of all IP traffic between SaNTA components
  – For peer authorization
  – For preventing man-in-the-middle and DoS attacks

• Integrity control of IP datagrams
• Prevention of IP replay attacks
• Confidentiality of original UDP datagrams encapsulated in ITL

• Possible integrations
  – Complex, SaNTA is an application, IPSec runs in OS kernels
4.3.6 Proposed Security Technologies

- **Peer authentication**
  - IPSec AH

- **Protection of data flows**
  - SSL between SaNTA peers for ITL handshakes and headers
  - SSL between SEs for original TCP payloads
  - IPSec ESP between SEs for original UDP payloads
  - UDP tunnel and IPSec ESP between SEs for other data flows (opaque)
4.3.6 Proposed Security Technologies
Secure TCP data flows
4.3.6 Proposed Security Technologies
Secure UDP data flows
4.3.6 Proposed Security Technologies
Secure “Opaque” data flows

<table>
<thead>
<tr>
<th>N1</th>
<th>SE1</th>
<th>IWU1</th>
<th>IWU2</th>
<th>SE2</th>
<th>N2</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP header (N1-N2)</td>
<td>IP header (SE1-IWU1)</td>
<td>IP header (IWU1-IWU2)</td>
<td>IP header (IWU2-SE2)</td>
<td>IP header (N1-N2)</td>
<td></td>
</tr>
<tr>
<td>AH header SA SE1-IWU1</td>
<td>AH header SA IWU1-IWU2</td>
<td>AH header SA IWU2-SE2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP header</td>
<td>UDP header</td>
<td>UDP header</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITL header (using UDP/IP address from SE1 &amp; SE2)</td>
<td></td>
<td></td>
<td>Original payload encapsulated in SE21-SE2 datagram (encrypted, ESP SE1-SE2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any payload</td>
<td></td>
<td></td>
<td></td>
<td>Any payload</td>
<td></td>
</tr>
</tbody>
</table>
4.3.7 Proposed key management: Authentication keys

- **Two possibilities, first is preferable**

  - **With asymmetric cryptography and X.509 certificates**
    - Possibly issued by a self-certified CA managed by a satellite link owner and SaNTA provider
    - Facilitates long-term authentication and authorization of a consistent set of SaNTA entities within several secure communication protocols
      - Examples: IPSec and SSL

  - **With secret, symmetric pre-shared keys**
    - Can be used to authenticate IPSec peers (SEs and IWUs)
    - Cannot be used to authenticate SSL peers (SEs)
    - Badly chosen passwords can be subject to off-line dictionary attacks
### 4.3.7 Proposed key management: Session keys

**Approach:**
- Give clients all the relevant tuning options
- This means that inter-SEs policies are client-defined

**Inter-SEs Authentication**
- For SSL sessions protecting TCP payloads
- **Client-defined possibilities:**
  - No authentication (anonymous Diffie-Helman)
  - X.509 certificate-based
### 4.3.7 Proposed key management: Session keys

- **Perfect Forward Secrecy (PFS)**
  - IKE SA must ensure
  - IPSec AH SAs don’t
  - Client defined:
    - IPSec ESP SA
- **Rekeying**
  - IKE and IPSec AH SAs don’t
  - Key refreshment is not critical
  - Client defined:
    - IPSec ESP SA used for UDP/opaque payloads
    - SSL used for TCP payloads