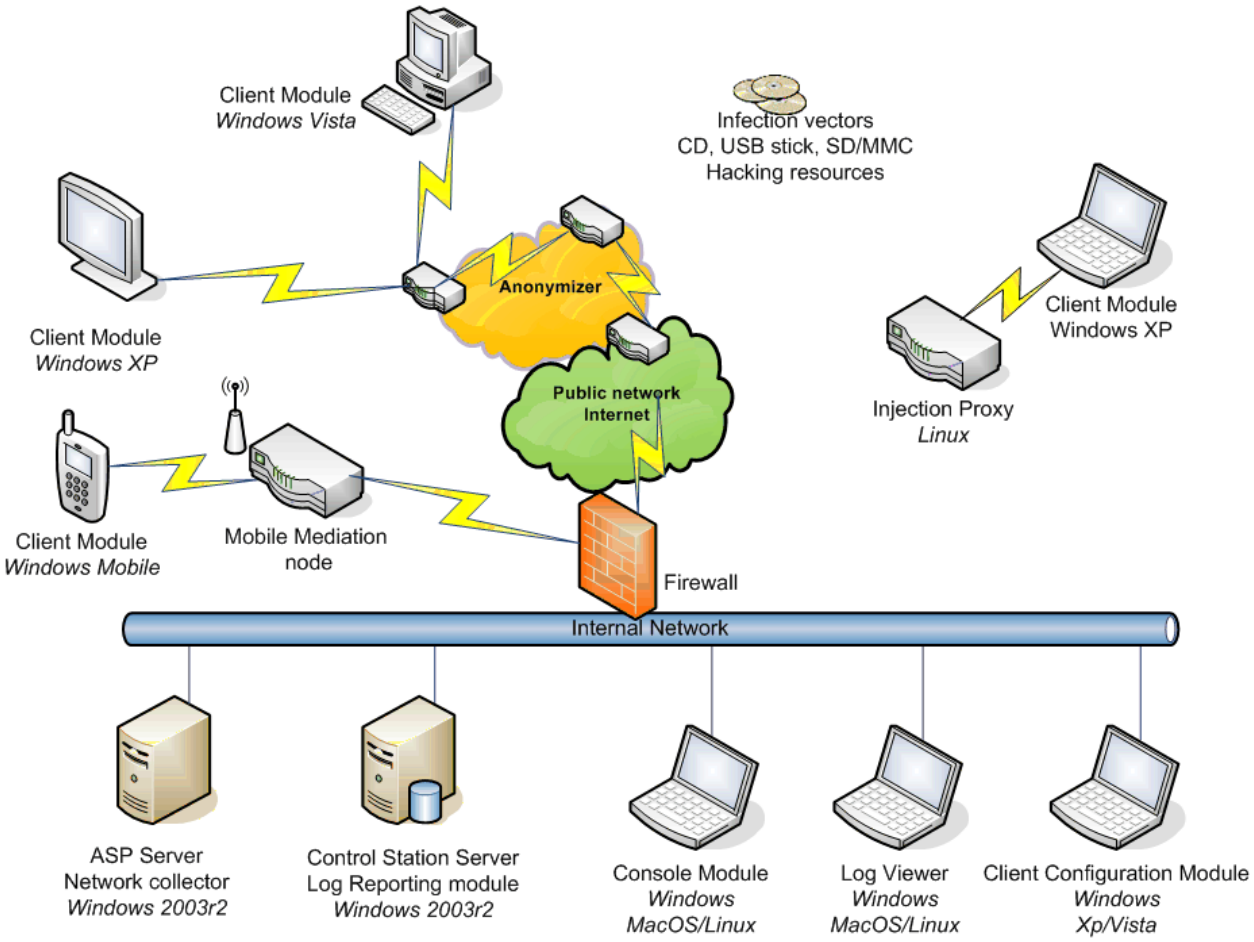
RCS SAT (Site Acceptance Test)

1. General

This document is a black-box compliancy test suite required for assessing the functional compliance of the Remote Control System software.
The provided suite of tests are intended to be used while delivering the solution at Customer's site (Site Acceptance Testing).

2. Architecture

The following image is just an example of a possible generic RCS infrastructure.
The real configuration at Customer's site depens on Customer's existing network and needs, along with the purchased RCS modules.



HT S.r.l.
Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

3. Naming conventions

Prior to run a batch of tests, it is suggested to get familiar with the following naming conventions, these are specifics to Remote Control System product.

- ✔ Backend Server (RCSDB)
- ✔ Network Collector (RCSASP)
- ✔ Console Module (RCSConsole)
- ✔ Client Module for Desktop (Windows)
- ✔ Client Module for Mobile (Symbian)
- ✔ Anonymizer

4. Testing scenario

Prior to run a batch of tests, it is required to setup a fully working testing environment, please refer to the Installation Guide using the following suggested scenario:

- ✔ Client Modules for any supported platform
- ✔ Server side setup, including Backend Server, Network Collector, Anonymizer network
- ✔ Console Module
- ✔ Infection media (USB stick, CD, SD card)

It is suggested to perform a preliminary test to assess the basic working functionalities of the system:

- ✔ Check network connectivity
- ✔ Open the Console Module to test connectivity with the Backend Server

HT S.r.l.
Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

5. Functional testing

This includes testing of product features for Remote Control System (both client and backend components).

User profiling

Scope: setup of supported user profiles in Remote Control System

1. **privilege separation**

Logon to Console using Administrator profile. Create new user with Administrator profile. Create new user with Tech profile. Create new user with Viewer profile. Test each user and validate results.	

Console Module (1)

Scope: testing of admin and tech user profiles and their capabilities

administrator

1. **activity**

Logon to Console using Administrator profile. Create a new activity. Validate results.	

2. **target**

Logon to Console using Administrator profile. Create a new target. Validate results.	

3. **audit logs**

Logon to Console using Administrator profile. View Remote Control System activity by accessing audit logs. Validate results.	

tech operator

1. **backdoor creation**

Logon to Console using Tech Operator profile. Create one backdoor for each platform to be tested. Validate results.	

HT S.r.l.
Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Console Module (2)

Scope: testing of backdoor configuration and infection vector building

TECH OPERATOR

1. **BACKDOOR CONFIGURATION**

For each backdoor to be tested, load the corresponding template configuration. Modify the synchronization server address (if needed). Validate results.	

2. **BACKDOOR BUILDING**

For each backdoor created, build all the available infection vectors. Validate results.	
Windows: build melted executable.	
Windows: build bootable CD.	
Symbian: build SIS installer.	

Network Collector

Scope: testing of Network Collector features

1. **WEB DECOY**

On a locally connected Target Windows PC point the web browser to the Network Collector ip address (HTTPS). It should be redirected to www.google.com. Validate results.	

HT S.r.l.
Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Client Module installation

Scope: Testing of target infection

1. **target infection**

Windows: infect a clean Windows 7 machine using the previously built infection vectors. Symbian: infect a clean Symbian S60v3 device using the previously build infection vector.	
Melted executable: run the infected executable on the target system. Verify invisibility to the user. Wait for data on the console.	
Bootable CD: boot the system with the previously built CD, infect the user. Wait for data on the console.	
SIS: install the package using the SIS installer. Wait for data on the console.	

Client Module to Server communication

Scope: testing of the supported synchronization channels Wait for the synchronization and validate results

1. **Internet (desktop)**

Connect previously infected Target Desktop PC to the Internet. Try to connect through anonymizer network. Network Collector IP address must be reachable by the target PC. Validate results using the console.	

2. **Offline retrieval (desktop)**

Boot an infected Target Desktop PC from CD or USB. Recover log files by exporting it on a USB media. Connect USB media to Network Collector. Drag and Drop the files to the repository. Validate results using the console.	

3. **Internet (mobile)**

Connect previously infected Target Mobile device to the Internet. Try to connect through anonymizer network. Network Collector IP address must be reachable by the target device. Validate results using the console.	

HT S.r.l.
Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

Console Module (3)

Scope: testing of viewer user profile, data browsing and end of activities

VIEWER OPERATOR

1. **VIEW LOGS**

Logon to the console using the Viewer Operator profile. Access to stored logs using dashboard functionalities. Validate results.	

2. **SEARCH PATTERN**

Logon to console using the Viewer Operator profile. Perform search selection on stored logs. Validate results.	

3. **EXPORT LOGS**

Logon to console using the Viewer Operator profile. Select relevant logs related to any activity. Add them to blotter. Export single log entries. Export whole blotter. Validate results.	

4. **SYSTEM HEALTH MONITOR**

Logon to console using the Viewer Operator profile. Check Remote Control System status using built in health monitor. Validate results.	

ADMINISTRATOR

1. **CLOSING THE ACTIVITY**

Close each created activity. Wait next synchronization of each infected device. Verify that all backdoors have been uninstalled (no more synchronizations will happen).	

HT S.r.l.
Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

DATE:

HT S.r.l.	**CUSTOMER**
_____	_____

HT S.r.l.
Via della Moscova, 13 20121 Milano
Tel: +39.02.29060603 – Fax: +39.02.63118946
P.IVA: 03924730967 – Capitale Sociale: € 223.572,00 i.v.
N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545