]HackingTeam[

RCS Certificates

Case Study

Contents

Important Notice

HT s.r.l. shall bear no responsibility or liability to a client or to any person or entity with respect to liability, loss or damage caused or alleged to be caused directly or indirectly by any HT s.r.l. product. This includes, but is not limited to, any interruption of service, loss of business or anticipatory profits or consequential damage resulting from the use or operation of any HT products. Information in this document is subject to change without notice and does not represent a commitment on the part of HT s.r.l. The systems described in this document are furnished under a license agreement or non-disclosure agreement.

All information included in this document, such as text, graphics, photos, logos and images, is the exclusive property of HT s.r.l. and protected by international copyright laws. Permission is granted to view and photocopy (or print) materials from this document for personal, non-commercial use only. Any other copying, distribution, retransmission or modification of the information in this document, whether in electronic or hard copy form, without the express prior written permission of HT s.r.l., is strictly prohibited. In the event of any permitted copying, redistribution or publication of copyrighted material, no changes in, or deletion of, author attribution, trademark legend or copyright notice shall be made.

1 Overview

RCS uses a variety of certificates to let the RCS Agents gather information on each device. Certificates are mandatory and cannot be avoided for proper functioning of RCS Agents.

NOTE	Symbian aside, all the certificate are provided by HT at no additional cost for the Customer.

Certificates are organized into three categories:

1. Certificates from an existing Certification Authority (**Type 1**)
2. Certificates with no identification information (**Type 2**)
3. Self-signed certificates (**Type 3**)

Type 1 certificates bear full details about the requestor, such as company name, address, technical contacts, and administrative contacts.

Type 2 certificates are uniquely bound to the requestor but no information is directly accessible. Information about the requestor can be asked to the Certification Authority that issued the certificate; sometimes that information is available via public databases as well.

Type 3 certificates are created by the software itself or by the Customer, and are self-signed. They bear no direct information about the requestor and, *unless* the same information is used (certification authority name, location…) each time a new certificate is created, there's no way to identify them as part of an RCS installation.

On specific architectures, more than one certificate may be required.

1.1 Symbian certificate

A Symbian Developer Certificate for up to 1000 IMEIs and 17 capabilities is required to install and run the RCS Agent on Symbian devices: this is due to the highly restricted nature of Symbian platforms. Unsigned applications haven't been allowed to run in any way starting from Symbian OS 9.1.
The Customer is required to buy a *Developer Certificate* from TrustCenter.

NOTE	The procedure to request a Symbian certificate and how to use it is detailed in the RCS manuals and provided as basic training upon purchase of the Symbian Platform.

2 Visibility

Information stored into certificates may be visibile to the Target. Two levels of visibility identify how much information the Target can access:

1. Certification information is not exposed without Target's intervention, but is accessible if the Target performs specific actions, for example browses the package properties.

2. Certification information may be obtained by extracting the signed binary from the RCS Agent, then performing further analysis on it. The certificate and its information are available only upon disclosure of the RCS Agent presence.

3 Architectures

Here is a list of all the supported RCS Agent architectures with their respective requirements for certificates:

Android

Type 3 certificate required.

BlackBerry

Type 2 certificate required.

iPhone

No certificate is required.

MacOS

No certificate is required.

Symbian

Type 2 certificate required after 21/Jun/2011, *type 1* certificate required for Agents signed before 21/Jun/2011.

Windows 32-bits

No certificate is required.

Windows 64-bits

type 1 certificate is required for kernel component.

Windows Mobile

Type 1 certificate is required for dropper

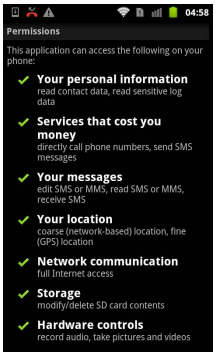
Type 3 certificate is required for Agent.

4 Analysis

Listed below is a risk analysis in case an Agent is identified, extracted and analysed.

4.1 Android

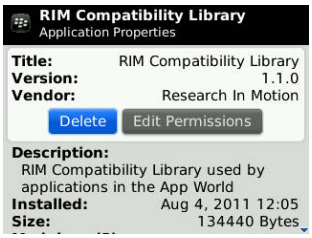
Certificate information is exposed only in case of a binary analysis of the Agent. A Type 3 certificate is currently provided by HT, thus disclosure of the Customer's identity is impossible.



4.2 BlackBerry

Certificate information is exposed only in case of a binary analysis of the Agent. T*ype 2* certificate is used, thus presenting no immediate danger of identification.

Currently the certificate is provided by HT, due to signing requirements during development process.



4.3 iOS (iPhone/iPad)

No certificate is used by the Agent on iOS platforms.

4.4 Mac OS X

No certificate is used by the Agent on OS X platforms.

4.5 Symbian

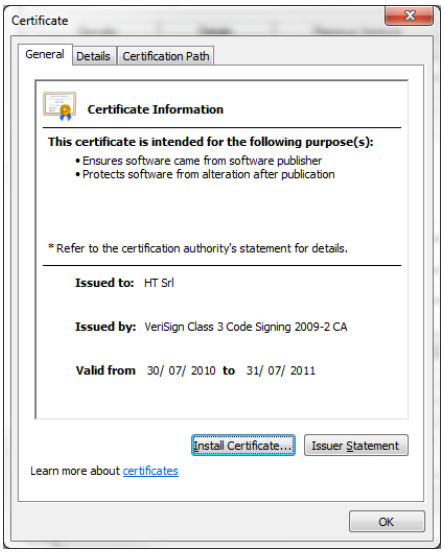
The Certificate information can be exposed by Target actions and by binary analysis of the Agent executable. *Type 2* certificate is used starting from 21st July 2011, posing no immediate risk of identification. Installations performed before 21st July 2011 uses *Type 1* certificates, thus showing identification information. Certificate is must be provided by the Customer.

4.6 Windows 32-bit

No certificate is used by the Agent on Windows 32-bit platforms.

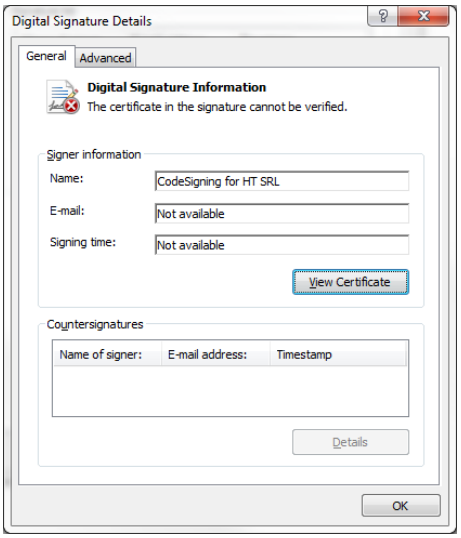
4.7 Windows 64-bit

The Certificate information can be exposed by Target actions and by binary analysis of the Agent executable. A T*ype 1* certificate containing company name and location information is used. Danger of identification is immediate if RCS or associated components are identified, extracted and analysed. Currently the certificate is provided by HT.



4.8 Windows Mobile

The Certificate information can be exposed by Target actions and by binary analysis of the Agent executable. T*ype 1* and T*ype 3* certificates are used. Danger of identification exists *only* at infection time. After this stage the component carrying *Type 1* certificate is erased from the system and only components using *Type 3* certificates are kept on the device.



5 Costs

Type 1 and T*ype 2* certificates must be acquired from Certification Authorities, the price may vary and there might be yearly subscription fees.

Android

Free.

BlackBerry

20 USD *una tantum*.

Symbian

200 USD, yearly fee.

Windows 64-bits

499 USD, yearly fee.

Windows Mobile

450 USD at subscription, 100 USD yearly fee or after signing 10 times.