ACKNOWLEDGEMENT

By utilizing this website and/or documentation, I hereby acknowledge as follows:

Effective October 1, 2012, QUALCOMM Incorporated completed a corporate reorganization in which the assets of certain of its businesses and groups, as well as the stock of certain of its direct and indirect subsidiaries, were contributed to Qualcomm Technologies, Inc. (QTI), a wholly-owned subsidiary of QUALCOMM Incorporated that was created for purposes of the reorganization.

Qualcomm Technology Licensing (QTL), the Company's patent licensing business, continues to be operated by QUALCOMM Incorporated, which continues to own the vast majority of the Company's patent portfolio. Substantially all of the Company's products and services businesses, including QCT, as well as substantially all of the Company's engineering, research and development functions, are now operated by QTI and its direct and indirect subsidiaries[1]. Neither QTI nor any of its subsidiaries has any right, power or authority to grant any licenses or other rights under or to any patents owned by QUALCOMM Incorporated.

No use of this website and/or documentation, including but not limited to the downloading of any software, programs, manuals or other materials of any kind or nature whatsoever, and no purchase or use of any products or services, grants any licenses or other rights, of any kind or nature whatsoever, under or to any patents owned by QUALCOMM Incorporated or any of its subsidiaries. A separate patent license or other similar patent-related agreement from QUALCOMM Incorporated is needed to make, have made, use, sell, import and dispose of any products or services that would infringe any patent owned by QUALCOMM Incorporated in the absence of the grant by QUALCOMM Incorporated of a patent license or other applicable rights under such patent.

Any copyright notice referencing QUALCOMM Incorporated, Qualcomm Incorporated, QUALCOMM Inc., Qualcomm Inc., Qualcomm or similar designation, and which is associated with any of the products or services businesses or the engineering, research or development groups which are now operated by QTI and its direct and indirect subsidiaries, should properly reference, and shall be read to reference, QTI.

[1] The products and services businesses, and the engineering, research and development groups, which are now operated by QTI and its subsidiaries include, but are not limited to, QCT, Qualcomm Mobile & Computing (QMC), Qualcomm Atheros (QCA), Qualcomm Internet Services (QIS), Qualcomm Government Technologies (QGOV), Corporate Research & Development, Qualcomm Corporate Engineering Services (QCES), Office of the Chief Technology Officer (OCTO), Office of the Chief Scientist (OCS), Corporate Technical Advisory Group, Global Market Development (GMD), Global Business Operations (GBO), Qualcomm Ventures, Qualcomm Life (QLife), Quest, Qualcomm Labs (QLabs), Snaptracs/QCS, Firethorn, Qualcomm MEMS Technologies (QMT), Pixtronix, Qualcomm Innovation Center (QuIC), Qualcomm iSkoot, Qualcomm Poole and Xiam.

Code Signing Management System Overview

80-V3999-1 B

Qualcomm Confidential and Proprietary

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, CA 92121-1714
U.S.A.

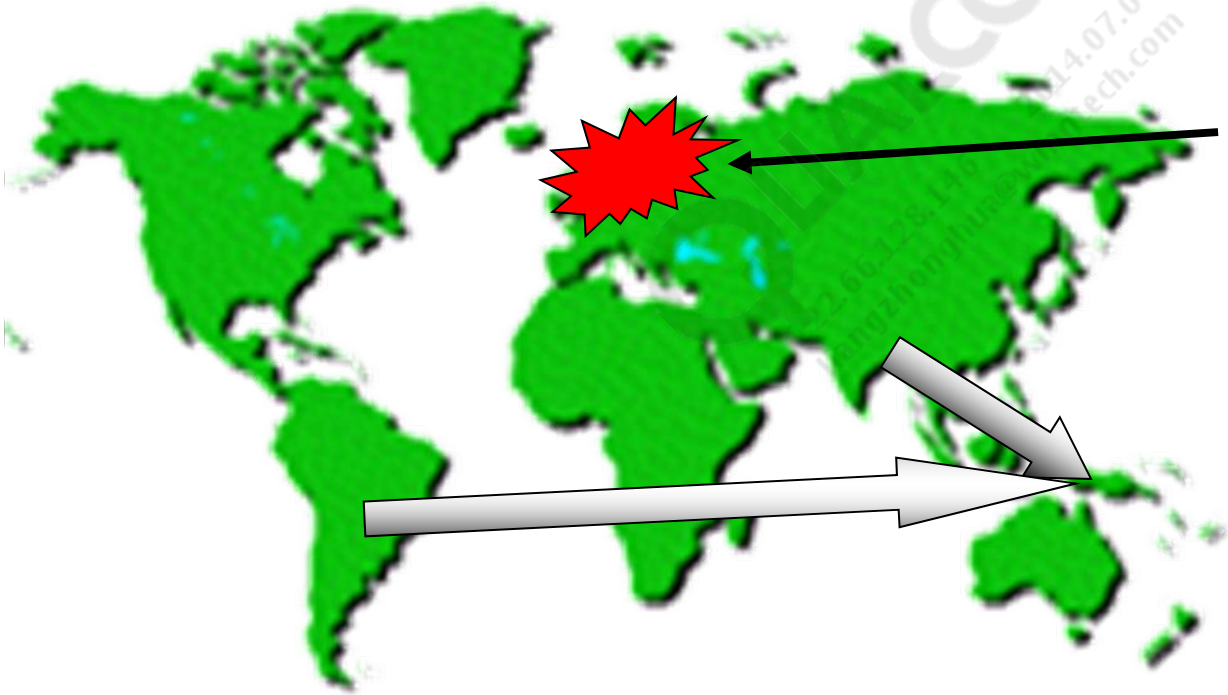
Revision History

Version	Date	Description
A	Jun 2005	Initial release
B	Mar 2010	Numerous changes were made to this document. It should be read in its entirety.

Contents

Phones are Attacked Everywhere, Everyday

Breaking “subsidy locks” is a big business



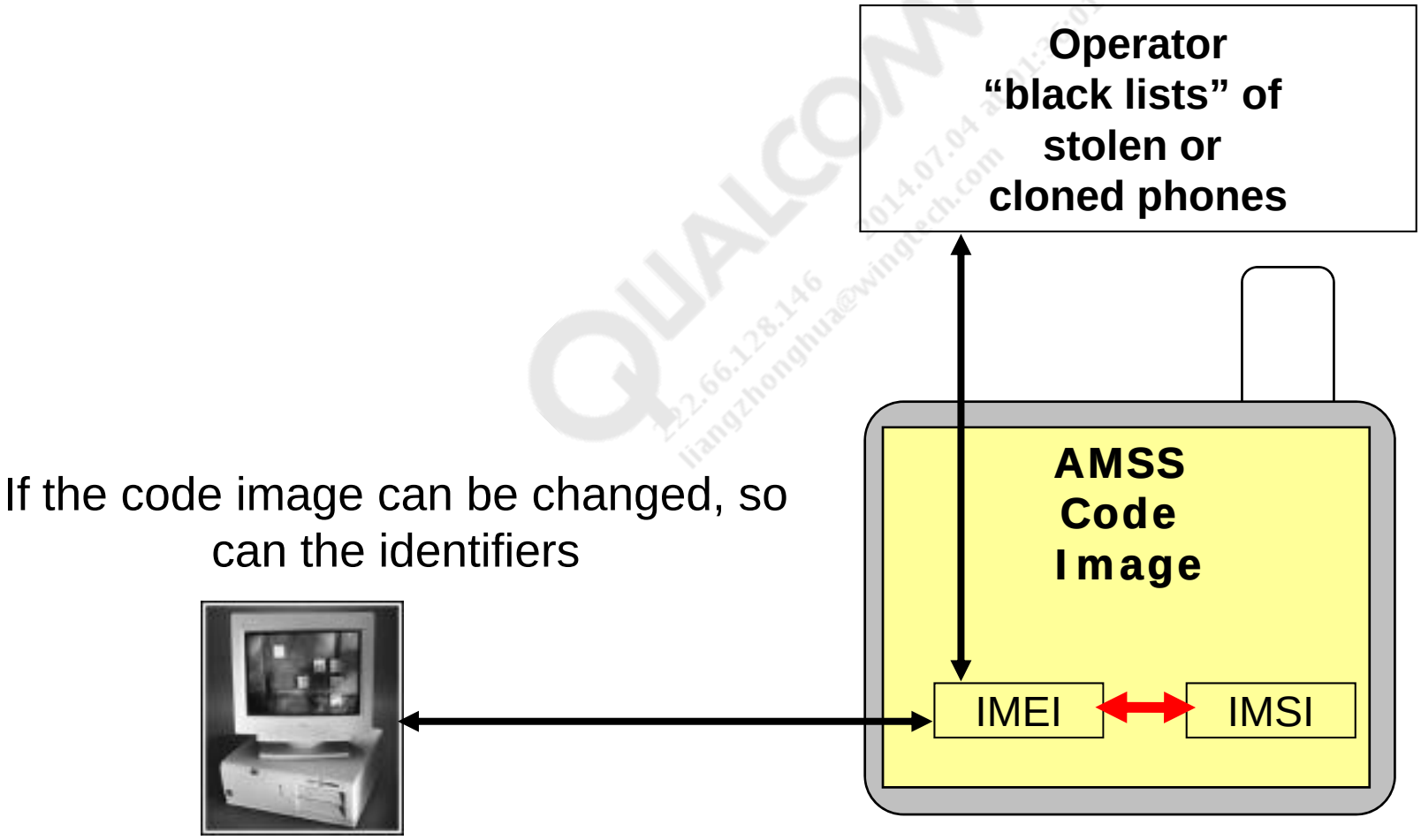
Phones are exported to other countries . . . taking a subsidized phone from, for example, one carrier to another carrier whose subscription is less expensive

Operators Mandate Better Security

Note: Operators lose millions of dollars every year due to fraud. Therefore, they mandate better security checks

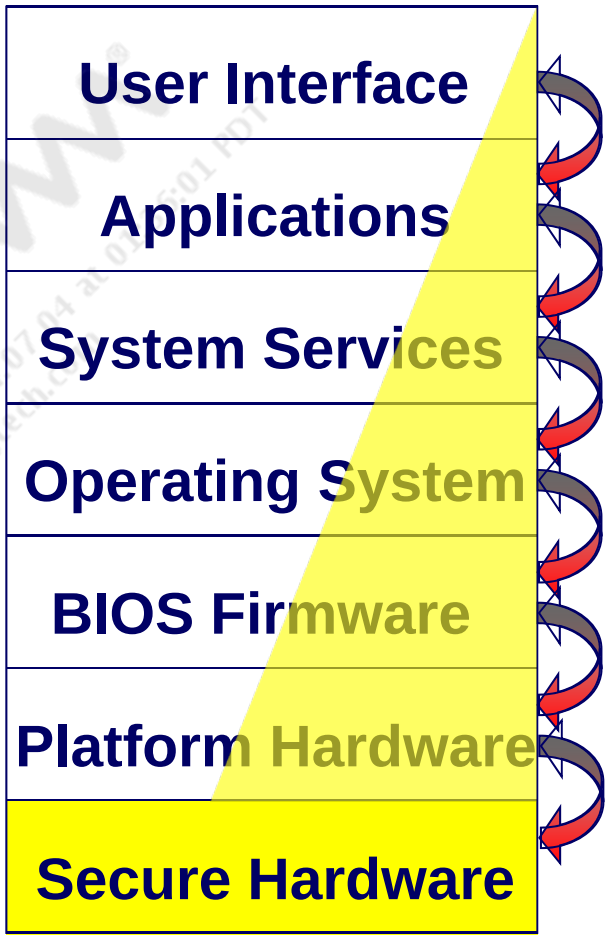
How Attackers Attack

- Breaking subsidy
- Stealing and cloning phones without being caught

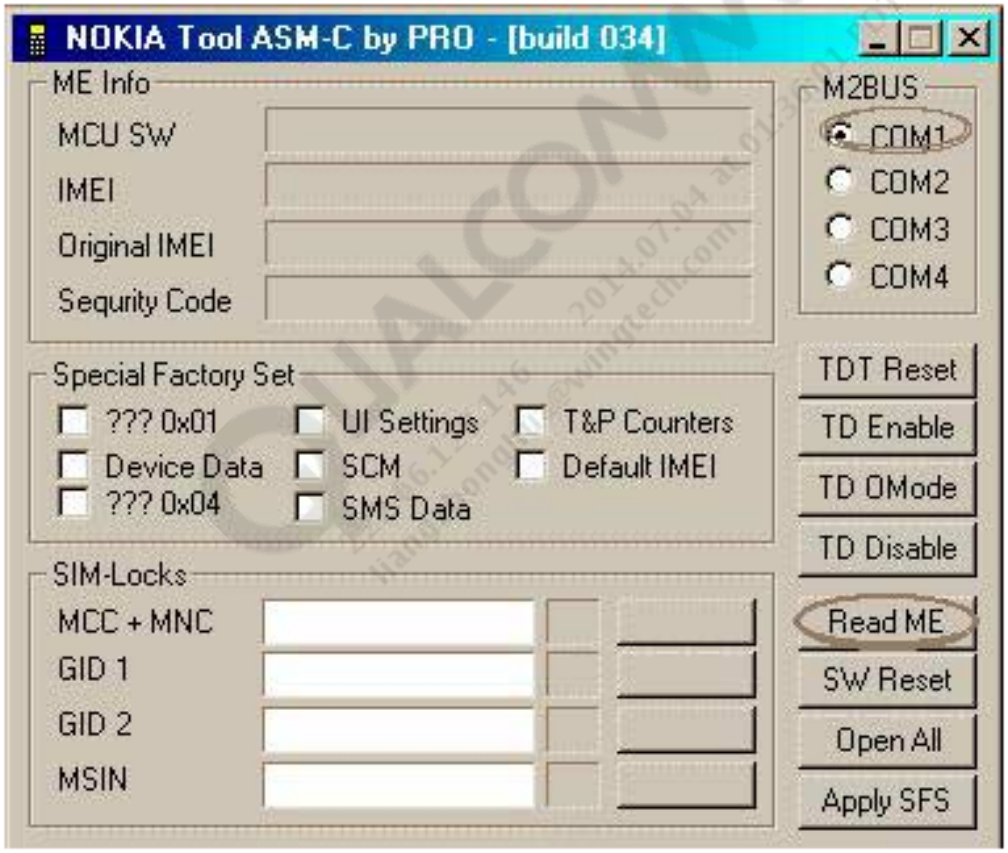


Market Demand – Hardware Security

- Security at any layer can be defeated by accessing the next lower layer
- Trusted computing requires security hardware as the foundation for platform security
- Trusted computing also requires security enablement features in each layer



Easily Available Online Tools Simplify and Automate the Process

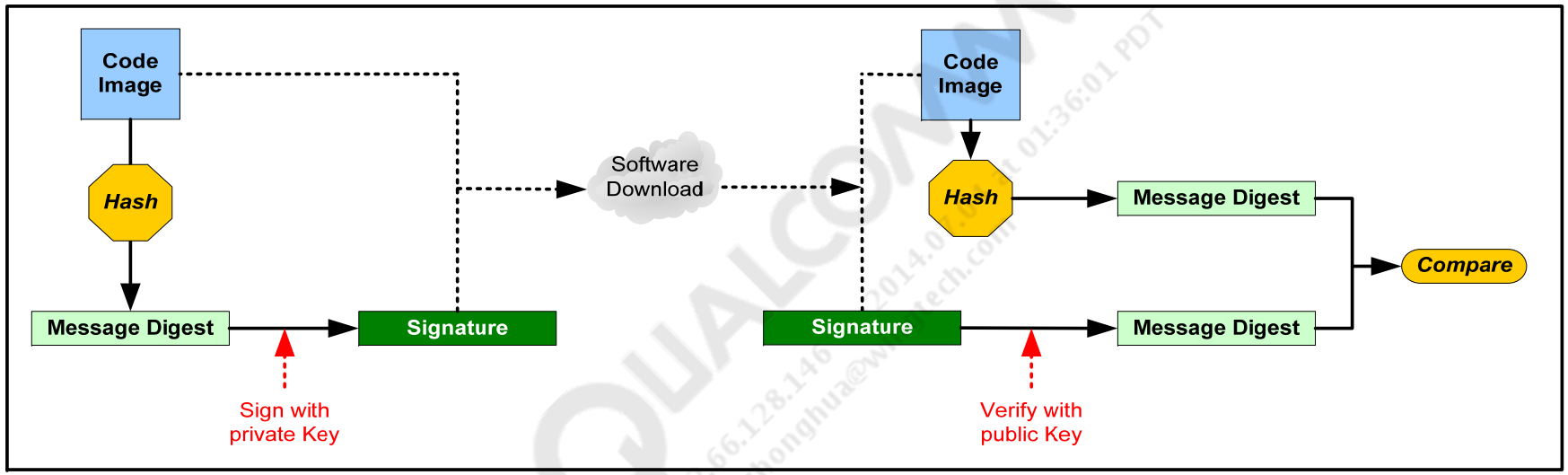


Once the port is configured correctly, click Read ME. The phone data will be filled in the fields of the tool. Next, click Open All and your phone will be free of all locks.

SecureMSM® Platform – The Three Pillars

- Secure boot
  - Ensures the device starts with known and trusted software
  - Data integrity and authenticity of code is verified every time the phone starts
  - Requires verification of the key and primary boot loader in order to be protected from modification
  - Is a countermeasure to protect against the most trivial “mom and pop” attacks
- Secure execution environment
  - Maintains the integrity of device at runtime
  - Memory separation keeps secret application data secret and protects applications from write attacks
  - Is a countermeasure against malware and network-based attacks at runtime
- Secure storage
  - Keeps confidential data (secrets) confidential
  - Examples are keys, pins, e-wallets, location data
  - Protects nonsecret data from modification, e.g., public keys, certificates

First Pillar – Secure Boot



Must be protected on MSM™ ASICs

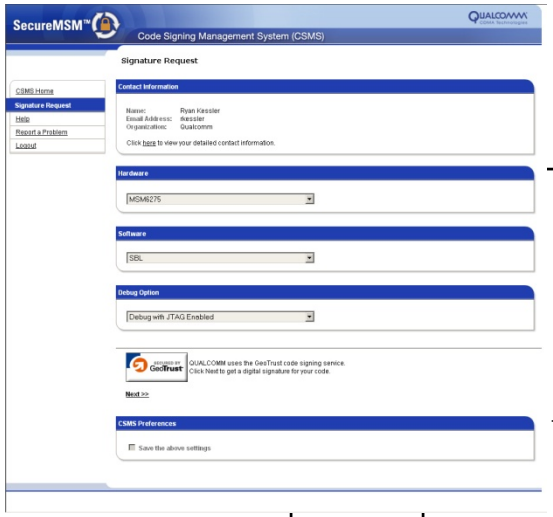
– MSM6250™ ASIC with $1 to $3 external Flash part

– MSM6280™, MSM6800™, QSC6055™, QSC6065™, QSC6075™, and QSC6085™ ASICs on ROM DIE

Public Key

Primary Boot Loader

Generate a Digital Signature



2. Create Message Digest (on Local PC)

GeoTrust

Message Digest

Secured Private Key

3. GeoTrust Signs MD with Private Key

Digital Signature

1. Log into QCOM CSMS portal

4. Download Digital Signature

Identity Cert

Final Code

Digital Signature

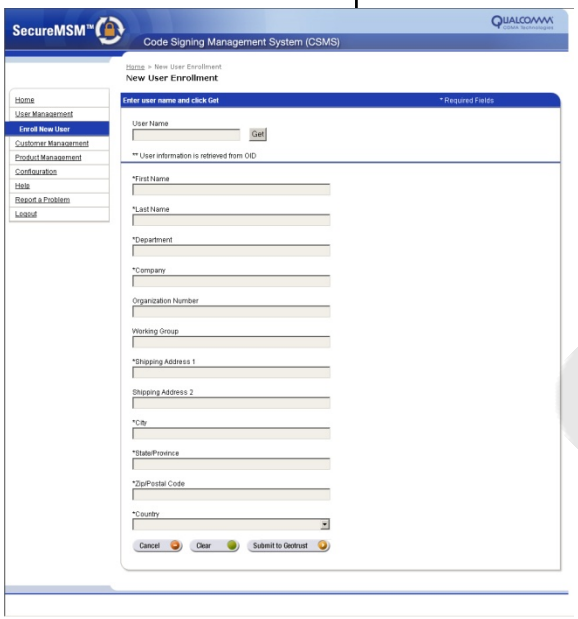
5. Customer Flashes Code Image and DS

AMSS Code Image

Digital Signature

Secure Boot Public Key

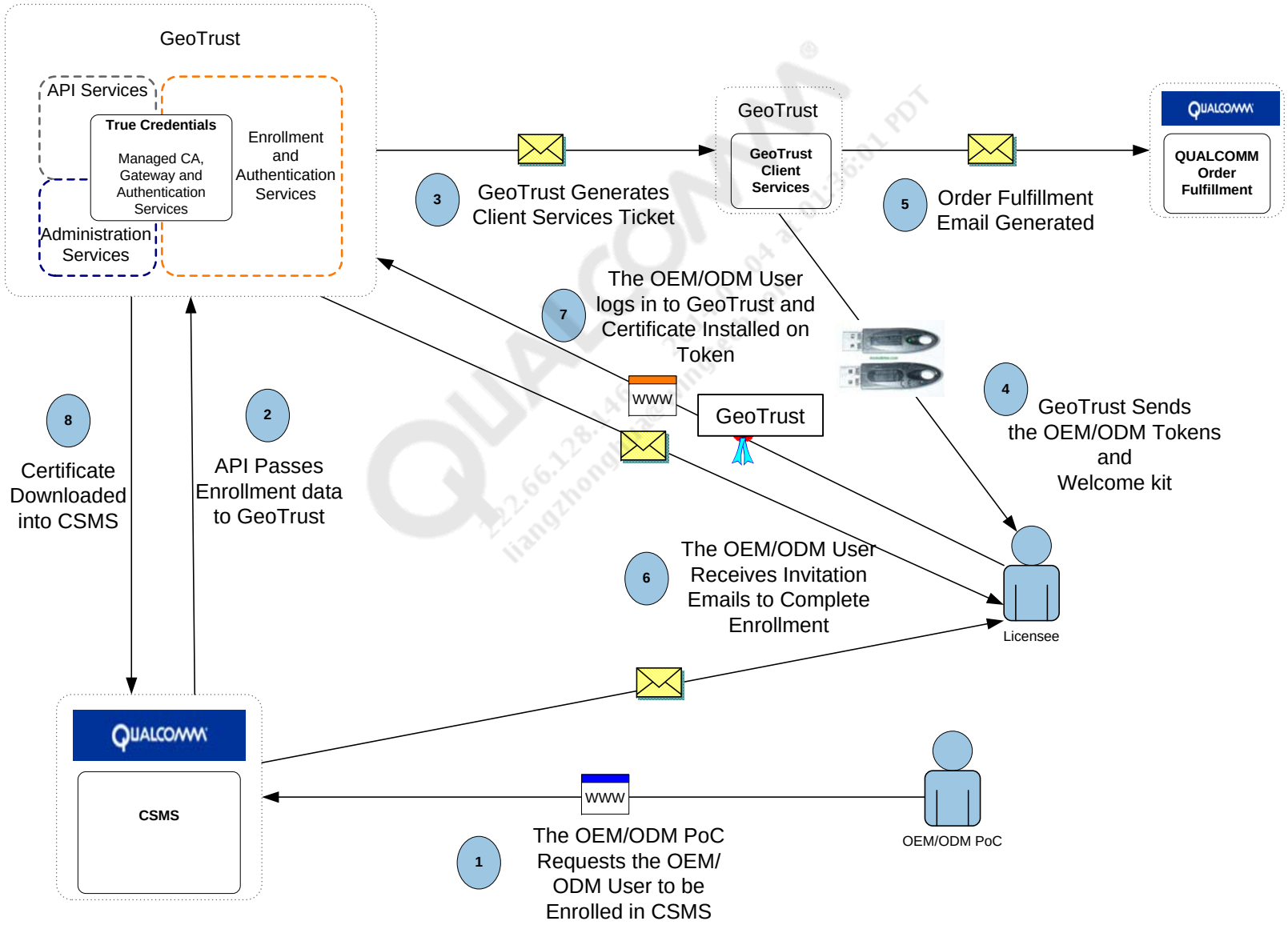
Administration of Code Signing Management System (CSMS)



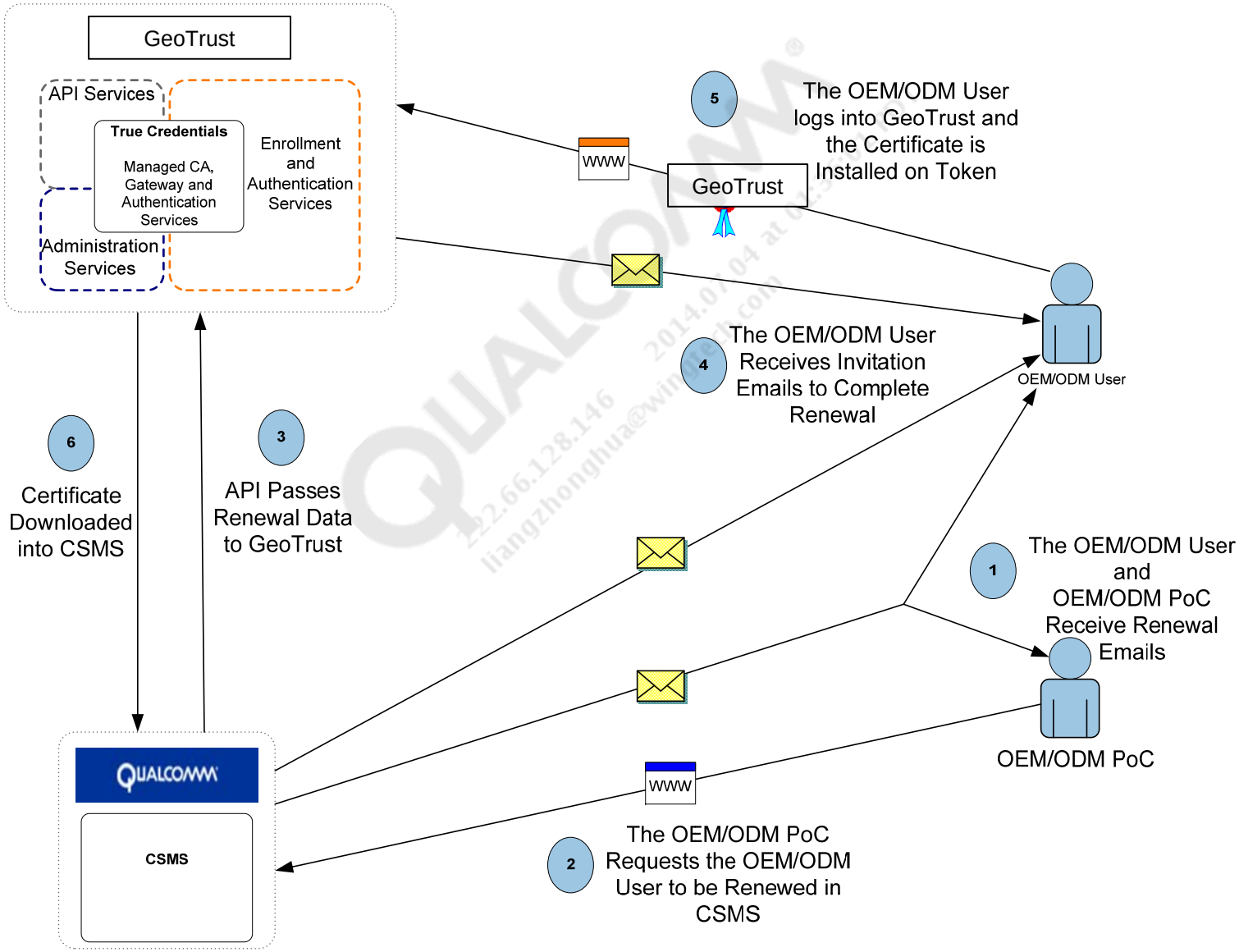
Customer Point of Contact

- A high-level customer point of contact shall be established by each licensee, who shall be responsible for:
  - All communications with the QCT CSMS Administrator (via CDMATech Support Salesforce cases) regarding the following:
    - New accounts, revocations, suspensions, and renewals
    - Requests for tokens
    - Password reset and reinitialization of accounts and/or tokens
  - Determining the number and method of distribution of tokens within his or her company
  - Tracking tokens and monitoring the number of certificates requested

Generating ID Certificates



Renewing ID Certificates



Requirements

- GeoTrust
  - There are no charges for generating a digital signature
  - Licensees pay a one-time fee of $549 per ID certificate
  - Licensees pay $399 for each ID certificate renewal
  - Maximum of one ID certificate per phone model (required)
  - Volume discounts in lots of 10
  - GeoTrust handles all logistics and billing
- Our licensees
  - We require an agreement to ensure that our licensees take full responsibility over their signed code
  - We vet each request and pass it to GeoTrust, who then performs all fulfillment, logistics, and billing

References

Ref.	Document	
Qualcomm		
Q1	*Application Note: Software Glossary for Customers*	CL93-V3077-1

Questions?

https://support.cdmatech.com