



CASE STUDY

QUALCOMM INCORPORATED

WIRELESS TELECOMMUNICATIONS
GIANT TRUSTS VERISIGN® CODE
SIGNING CERTIFICATE TO PROTECT
ITS KEY DEVELOPMENT PLATFORM





CASE STUDY

In 2001, QUALCOMM Incorporated introduced Binary Runtime Environment for Wireless (BREW®) as a comprehensive, open development platform for the creation of mobile phone applications. With competition driving down cellular call profit margins, many carriers saw wireless application services as a strong new source of revenue. In addition to rich content development and delivery capabilities, BREW immediately differentiated itself by providing an interface between the application and the wireless device on-chip operating system. This facility gave programmers the ability to develop applications without needing to include code for each individual cellular device or write multiple system interfaces. Developers were strongly attracted by this capability and it proved equally compelling for manufacturers by allowing access to the most popular applications for their whole range of current and future devices.

PROTECTING THE DEVELOPMENT ENVIRONMENT

In 2000, before launching the BREW platform, QUALCOMM was concerned about operational physical security for the root key—including limiting the number of copies—and validating developer access. The QUALCOMM team responsible for BREW did not have the manpower or resources to create and deploy in-house solutions to address these security concerns.

Martin Bennett, QUALCOMM’s senior manager of IT, explained, “If an unauthorized developer gained access and put a sub-standard application out there—or worse still, some type of malicious code—that caused problems for our operators, there would be a huge negative impact on the trust that we have built with our partners—potentially doing untold damage to QUALCOMM’s reputation and business. We therefore wanted the notarization of developers to occur every time the code is touched.”

QUALCOMM opted to utilize code signing certificates, mandating that the developer signs all code with the same digital signature using public key infrastructure (PKI) cryptography.

The QUALCOMM BREW team understood that security of the root key was mission critical for the long-term success of the platform and consequently looked to outsource the management of code signing and developer notarization to a trusted and proven vendor. In 2001, VeriSign won the selection process.

VERISIGN’S FLEXIBLE PKI SOLUTIONS

VeriSign® Code Signing Certificate, together with some custom code, was implemented to accomplish the physical security operations relating to storage of the BREW root key. Matthew Hohlfeld, staff engineer, elaborated, “This approach ensures that VeriSign authenticates the source of all requests from our company; cross-checking the applicant against the list of people that QUALCOMM says are approved to make that particular request.”

SOLUTION SUMMARY:

Wanting notarization of developers to occur every time they access code within the BREW® environment and also needing robust root key security, QUALCOMM elected to leverage VeriSign® Code Signing Certificates and has since successfully defended the code from all unauthorized developer access.

Industry

- Telecommunications

Challenges

- It was critical to ensure that the BREW environment did not allow the company’s high standards of trust and integrity to be open to compromise.
- Needed operational physical security for the BREW root key.
- All developers accessing the code base needed to be validated and authorized.

Solution

- VeriSign® Code Signing Certificate
- VeriSign® Document IDs for BREW®
- VeriSign Platinum support

Results

- There has not been a single unauthorized developer security breach.
- The BREW root key is appropriately secured.
- A notarized, time-stamped record is created for all code changes within the environment, creating an auditable history of all activities.





CASE STUDY

The VeriSign Code Signing Certificate solution performs a digital packaging of code and content, which protects software publishers and users when they download code over the Internet or mobile networks. Digital signatures authenticate the source and verify the integrity of content.

Secondly, for the certification of third-party BREW authenticated developers, QUALCOMM and VeriSign collaborated to create and deploy a customized version of the solution, known as VeriSign® Document IDs for BREW®. Hohlfeld described the steps in the operational process, “Via submission from a custom VeriSign portal, a new developer goes through Class Two or Three authentication with VeriSign where the corporate identity of the developer is cross-checked. Once successfully validated, VeriSign issues certificates for key material so the developer can authenticate back with QUALCOMM. Having validated with QUALCOMM, the developer gets a tool that interoperates with the key material provided by VeriSign, and this then allows them to sign code for submission to QUALCOMM’s BREW platform.”

VeriSign Document IDs for BREW enables authorized BREW developers to digitally notarize BREW applications from their own desktop, giving them non-repudiable proof of document content, source, together with a time-stamp, and in turn QUALCOMM is assured of the content source and integrity.

The third element to QUALCOMM’s security solution is digital notarization. “This is an Internet RFC 3161-based time-stamping service from VeriSign,” said Hohlfeld, “so when QUALCOMM submits a signed request that’s appropriately labeled, VeriSign returns a specialized formatted version.”

To round out the VeriSign solution QUALCOMM has Platinum support providing service availability at 99.5 percent around the clock. “We have a good handle on our business processes and how they are complemented by the VeriSign solution—we’ve optimized the support and consulting services to match these requirements,” noted Bennett. “VeriSign has been very receptive to any requests that we’ve had, and we have monthly meetings with the support team to track and progress action items that need resolution. We have a large number of developers—currently more than 1,800—doing testing along with a third-party test house, and by using VeriSign’s Platinum support, we have strong peace of mind.”

TRUSTING IN VERISIGN

Today, QUALCOMM is undertaking a review and possible migration of its certification of third-party BREW authenticated developers to the Authenticated Content Signing (ACS) platform. Jane Bushor, program manager, commented, “We are currently defining how to optimally transition to ACS; there are some hurdles, but by collaborating with VeriSign, we’re confident that we can make this project as successful as our current solutions have been.”

“Since going live we have not had a single unauthorized developer breach our security, which is why our relationship with VeriSign is so strong and long-standing... We have an inherent trust in VeriSign to protect us.”

Martin Bennett,
senior manager of IT,
QUALCOMM Incorporated





CASE STUDY

The success of VeriSign's security solutions has been proven by QUALCOMM experiencing zero "Severity 1" security events. Bennett reflected, "Since going live, we have not had a single unauthorized developer breach our security, which is why our relationship with VeriSign is so strong and long-standing. It's been a rewarding and easy partnership to maintain."

He concluded, "We have an inherent trust in VeriSign to protect us."

Visit us at www.Verisign.com for more information.

Opinions expressed here are those of the original speakers, and not necessarily of VeriSign.

©2009 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, the Checkmark Circle logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign, Inc., and its subsidiaries in the United States and foreign countries. All other trademarks are property of their respective owners.

00027415 11-16-2009

