

ÉTUDE DE CAS

QUALCOMM INCORPORATED

LE GÉANT DES TÉLÉCOMMUNICATIONS
SANS FIL MISE SUR LES CERTIFICATS
VERISIGN® CODE SIGNING POUR PROTÉGER
SA PLATE-FORME DE DÉVELOPPEMENT.





ÉTUDE DE CAS

En 2001, QUALCOMM Incorporated lance Binary Runtime Environment for Wireless (BREW®), une plate-forme de développement ouverte et complète pour la création d'applications de téléphonie mobile. La concurrence entraînant la baisse des marges bénéficiaires sur le prix des communications, de nombreux opérateurs voient alors dans les services applicatifs sans fil un nouveau gisement de valeur important. Outre un champ étendu de possibilités en matière de développement et de livraison de contenus enrichis, la plate-forme BREW se démarque immédiatement par son interface entre l'application et le système d'exploitation sur puce du combiné mobile. Résultat : les développeurs sont vite séduits par cette nouvelle plate-forme qui leur permet de programmer des applications sans devoir y inclure du code pour chaque terminal mobile, ni écrire plusieurs interfaces système. Les fabricants ne tardent pas à leur emboîter le pas, convaincus des avantages d'un accès aux applications les plus répandues sur toute leur gamme de téléphones actuels et futurs.

UN ENVIRONNEMENT DE DÉVELOPPEMENT PROTÉGÉ

En 2000, avant le lancement de BREW, la société QUALCOMM se trouve confrontée à un problème de sécurité physique opérationnelle de la clé racine, notamment en termes de limitation du nombre de copies et de validation de l'accès des développeurs. L'équipe projet BREW ne dispose alors pas du personnel ni des ressources nécessaires pour créer et déployer en interne des solutions à ces questions de sécurité.

Martin Bennett, Responsable informatique QUALCOMM, présente ainsi les risques encourus à l'époque : « Si un développeur non autorisé réussissait à accéder à la plate-forme et à y placer une application de mauvaise qualité ou, pire encore, du code malveillant susceptible d'entraîner des problèmes chez nos opérateurs, les répercussions sur les relations de confiance établies avec nos partenaires auraient pu causer des dommages inestimables à la réputation et à toute l'activité de QUALCOMM. Nous souhaitons donc qu'une notarisation des développeurs soit mise en place à chaque modification du code. »

QUALCOMM opte alors pour les certificats de signature de code. La raison ? Avec ces certificats, un développeur signe obligatoirement tout le code en utilisant la même signature numérique basée sur la cryptographie PKI (Public Key Infrastructure).

Ne tardant pas à saisir l'enjeu majeur de la sécurité de la clé racine pour la pérennisation de sa plate-forme, l'équipe QUALCOMM BREW cherche alors à confier la gestion de la signature de code et de la notarisation des développeurs à un prestataire d'expérience et de confiance. En 2001, la société VeriSign remporte l'appel d'offre.

SOLUTIONS PKI : LA FLEXIBILITÉ SIGNÉE VERISIGN

Une solution associant les certificats VeriSign® Code Signing à du code développé en interne est rapidement mise en œuvre pour exécuter les opérations de sécurité physique liées au stockage de la clé racine BREW. Matthew Hohlfeld, ingénieur logiciel, témoigne : « Grâce à cette approche,

SYNTHÈSE DE LA SOLUTION :

QUALCOMM souhaitait d'une part mettre en place une notarisation des développeurs à chacun de leur accès à du code au sein de l'environnement BREW®, et d'autre part garantir la sécurité de la clé racine. Le géant des télécoms a donc opté pour les certificats VeriSign® Code Signing. Depuis, l'entreprise protège efficacement son code contre tout accès par des développeurs non autorisés.

Secteur d'activité

- Télécommunications

Défis majeurs

- Lancement de l'environnement BREW sans remise en cause du capital fiabilité et intégrité de l'entreprise.
- Mise en place de la sécurité physique opérationnelle de la clé racine BREW.
- Mise en œuvre d'un processus de validation et d'autorisation de tous les développeurs accédant à la base du code.

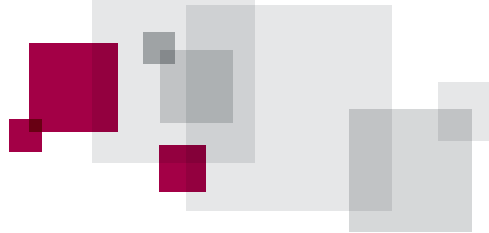
Solution

- Certificats VeriSign® Code Signing
- -VeriSign® Document IDs for BREW®
- Assistance VeriSign Platinum

Résultats

- Aucun développeur non autorisé n'a porté atteinte à la sécurité du code.
- La clé racine BREW est parfaitement sécurisée.
- Un enregistrement horodaté est notarié pour chacune des modifications de code au sein de l'environnement, avec à la clé la traçabilité de toutes les activités.





ÉTUDE DE CAS

VeriSign authentifie la source de toutes les demandes internes et vérifie par recoupement que la personne est bien autorisée par QUALCOMM à faire la demande en question. »

En premier lieu, la solution VeriSign Code Signing procède à un conditionnement numérique du code et du contenu. Le but ? Protéger les éditeurs de logiciels et les utilisateurs lorsqu'ils téléchargent du code sur Internet ou sur les réseaux mobiles. Les signatures numériques authentifient la source et garantissent l'intégrité du contenu.

Ensuite, pour la certification de développeurs externes authentifiés BREW, QUALCOMM et VeriSign ont collaboré à la création d'une version personnalisée de la solution, baptisée VeriSign® Document IDs for BREW®. Matthew Hohlfeld revient sur les différentes étapes de la procédure : « Via un portail VeriSign propre à QUALCOMM, tout nouveau développeur passe par une authentification de classe 2 ou 3 effectuée par VeriSign, qui vérifie son identité par recoupement. Après validation, VeriSign émet des certificats pour les documents clés, afin que le développeur puisse s'authentifier auprès de QUALCOMM. Après validation par QUALCOMM, le développeur obtient un outil interopérable avec les documents clés fournis par VeriSign. Il est ainsi habilité à signer du code avant soumission à la plate-forme BREW de QUALCOMM. »

VeriSign Document IDs for BREW permet aux développeurs BREW autorisés de notariser numériquement les applications BREW depuis leur station de travail, fournissant ainsi une preuve irréfutable du contenu et de la source du document, ainsi qu'un horodatage. Grâce à ce système, QUALCOMM ne peut nourrir aucun doute quant à la source et à l'intégrité du contenu.

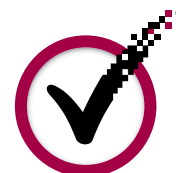
La notarisation numérique constitue le troisième pilier de la solution de sécurisation QUALCOMM. « Avec le service d'horodatage VeriSign basé sur la norme Internet RFC 3161, quand QUALCOMM soumet une demande signée et étiquetée de façon appropriée, VeriSign renvoie une version spécialement formatée. » ajoute Matthew Hohlfeld.

Pour compléter la solution VeriSign, QUALCOMM dispose d'une assistance Platinum qui assure un niveau de disponibilité à 99,5 %, 24h/24. « Nous maîtrisons parfaitement nos processus métier et la manière dont la solution VeriSign s'inscrit dans leur prolongement. Nous avons optimisé les services d'assistance et de conseil en tenant compte de nos exigences », remarque Martin Bennett. « La société VeriSign a été très réceptive à nos différentes requêtes, et nous nous réunissons tous les mois avec l'équipe d'assistance pour faire un point sur l'état d'avancement et le suivi des questions à résoudre.

Nous comptons un grand nombre de développeurs, plus de 1 800 actuellement, qui effectuent leurs tests en conjonction avec un prestataire spécialisé. L'assistance Platinum VeriSign nous offre en ce sens un gage de sérénité. »

« Depuis l'implémentation, nous n'avons pas connu une seule faille de sécurité causée par un développeur non autorisé. C'est pourquoi nos relations avec VeriSign sont si étroites et durables... Nous accordons une confiance totale à VeriSign pour notre protection. »

Martin Bennett,
Responsable informatique,
QUALCOMM Incorporated





ÉTUDE DE CAS

VERISIGN : EN TOUTE CONFIANCE

Aujourd'hui, QUALCOMM envisage une migration de sa certification de développeurs authentifiés BREW tiers vers la plate-forme ACS (Authenticated Content Signing). Comme l'indique Jane Bushor, responsable de programme : « Nous étudions actuellement diverses pistes de transition vers ACS. Il existe certes certains obstacles, mais avec la collaboration de VeriSign, nous sommes convaincus de pouvoir faire de ce projet une aussi belle réussite que les solutions actuelles. »

L'efficacité des solutions de sécurisation VeriSign est prouvée : QUALCOMM n'a connu à ce jour aucun événement de gravité de niveau 1. Martin Bennett témoigne : « Depuis l'implémentation, nous n'avons pas connu une seule faille de sécurité causée par un développeur non autorisé. C'est pourquoi nos relations avec VeriSign sont si étroites et durables. Ce partenariat fécond s'entretient de lui-même. »

Et de conclure : « Nous accordons une confiance totale à VeriSign pour notre protection. »

Pour plus d'informations, consultez notre site à l'adresse www.Verisign.fr

« Depuis que nous avons mis en place le service VIP FDS, associé à une couche de sécurité plus manuelle en arrière-plan, nous avons déjà constaté une baisse tangible des activités néfastes. À ce jour, nous n'avons subi AUCUNE perte de fonds. Toutefois, la prudence reste de mise et nous sommes en permanence à la recherche de nouvelles pistes d'amélioration. Ainsi, nous envisageons actuellement l'authentification multifactorielle pour réduire davantage les tentatives de fraude. Notre cahier des charges stipulait en outre une exigence de fiabilité à 100 % des transmissions de mots de passe à usage unique, où que nos membres se trouvent lorsqu'ils accèdent à leur compte. »

Blanca Guerrero, Directeur des systèmes d'information, Addison Avenue Federal Credit Union

Les opinions exprimées ici sont celles des personnes qui les ont émises, et pas nécessairement celles de VeriSign.

©2010 VeriSign Sarl. Tous droits réservés. VeriSign, le logo VeriSign, le cercle coché et les autres marques commerciales, marques de services et logos sont des marques commerciales déposées ou non de VeriSign et de ses filiales aux États-Unis et dans d'autres pays. Toutes les autres marques citées appartiennent à leurs détenteurs respectifs.

00028632 07-04-2010
ZE4482

