Prolongation de la durée de vie des certificats TLS STCA SHA-1

Contexte

La fonction de hachage SHA-1, utilisée dans de nombreux contextes, est très fragilisée par plusieurs attaques publiquement documentées. En raison de ces faiblesses connues, son utilisation dans un contexte sécuritaire est très fortement déconseillée depuis 2011 par les agences étatiques (ANSSI[1], NIST[2]). A la même date, son utilisation pour la signature de certificats numériques a été interdite par PCI dans le standard PCI PTS v3[3]. Cette interdiction a ensuite été élargie à tous les contextes sécuritaires couverts par PCI DSS[4] en 2017.

PayCert, qui opère l'autorité de certification STCA, a annoncé en avril 2016 la fin de l'émission des certificats signés avec la fonction SHA-1 et la création d'une nouvelle racine dont les certificats sont signés avec une fonction de la famille SHA-2 (SHA-256). Les derniers certificats dits « SHA-1 » devaient être émis avant le 31 décembre 2018, pour une fin de validité fixée au plus tard au 31 décembre 2020.

Cette migration prévue de longue date dépend cependant fortement de la migration du parc d'acceptation existant. En effet, les systèmes d'acceptation évalués selon les standards antérieurs à PCI PTS v3 (par exemple PED v1, PED v2), ne disposent pas nécessairement de la fonction SHA-256. Cette absence de support les empêche donc de se connecter à un serveur présentant un certificat récent, rendant ainsi le terminal inopérant. Il est donc essentiel que ces systèmes d'acceptation soient mis à jour lorsque cela est possible, ou remplacé par des systèmes d'acceptation plus récents.

Début 2020, le nombre de systèmes d'acceptation ne supportant pas SHA-256 représentait encore une part significative du parc d'acceptation CB. Pour éviter une interruption de service, et compte tenu du contexte sanitaire et des efforts de migration restant à faire, CB a accepté de déroger au calendrier défini avec PayCert et de renouveler exceptionnellement les certificats « SHA-1 » jusqu'au 30 juin 2020, avec une durée de validité d'un an. Ces certificats arrivent donc à expiration au plus tard au 30 juin 2021.

Cependant, le contexte sanitaire a complexifié les opérations de migration. De très nombreux commerces ont été fermés ou sont toujours fermés et leurs systèmes d'acceptation ne peuvent donc pas être migrés. Il y a un réel risque qu'une fois ces commerces rouverts, à l'été 2021, ils ne puissent

[1] https://www.ssi.gouv.fr/uploads/2012/09/NT_IPsec.pdf
[2] https://csrc.nist.gov/projects/hash-functions/nist-policy-on-hash-functions
[3] https://www.pcisecuritystandards.org/documents/PTS_POI_Technical_FAQs_v3_July_2013.pdf
[4] https://blog.pcisecuritystandards.org/how-the-sha-1-collision-impacts-security-of-payments

plus accepter de paiements par carte avec leurs systèmes d'acceptation non migrés. En mars 2021 le risque d'interruption de service demeure donc important.

CB va donc permettre aux porteurs de certificats « SHA-1 » de les renouveler pour une année supplémentaire, fixant la nouvelle date de fin de vie de ces certificats à juin 2022. Cependant, plusieurs conditions doivent être réunies pour que ce renouvellement soit autorisé.

Conditions pour le renouvellement

Les porteurs de certificats « SHA-1 » souhaitant les renouveler doivent formuler une demande écrite à CB dans laquelle :

- Ils fournissent des informations précises sur le parc restant à migrer (nombre de systèmes d'acceptation, typologie des systèmes non migrés)
- Ils s'engagent et détaillent un planning détaillé de migration
- Ils s'engagent à fournir trimestriellement à Frenchsys le nombre de systèmes d'acceptation migrés depuis ce renouvellement, et le nombre de systèmes d'acceptation restant à migrer avant le 30 juin 2022. Ces rapports devront être fournis au plus tard le 10 du mois (10 octobre 2021, 10 janvier 2021, 10 avril 2021)

Ces demandes de dérogations prendront la forme d'un courrier officiel sur papier à entête, adressées en pièce jointe par courriel à Emmanuel le Chevoir (emmanuel-le-chevoir@cartes-bancaires.com).

Les rapports de suivi trimestriel seront transmis par courriel à Jean-Marc Chénais (jean-marc.chenais@frenchsys.com)

Note rédigée par : Emmanuel le Chevoir
Date de publication : 20 avril 2021
Référence de la note : DPE-ESS-NTE-2021-02
Révision : 1.2