STCA : SHA-2

Dans le cadre des récentes évolutions des exigences sécuritaires CB, et notamment en ce qui concerne l'utilisation de l'algorithme SHA-1, certains travaux sont actuellement en cours sur la plate-forme STCA afin de migrer vers une nouvelle AC complètement basée sur des empreintes utilisant l'algorithme de hachage SHA-2 (ou SHA-256).

Cette migration comporte 2 volets. Le premier volet permettra la génération de certificats serveurs STCA avec empreinte SHA-2, tout en conservant les clés racines actuelles. Ces certificats serveurs STCA seraient alors compatibles avec le parc de terminaux actuels (c'est-à-dire potentiellement sans nouveau déploiement de certificat racine d'AC STCA).

Le second volet, consistera à mettre en place une nouvelle AC STCA avec signature reposant entièrement sur du SHA-2 et avec de nouvelles clés racines d'AC. Un nouveau certificat racine d'AC sera alors généré et devra être progressivement diffusé sur le terrain.

Des certificats de tests pour les deux nouvelles configurations pourront être délivrés dès Juin 2016. Les certificats de productions pourront être délivrés à partir de Juillet 2016.

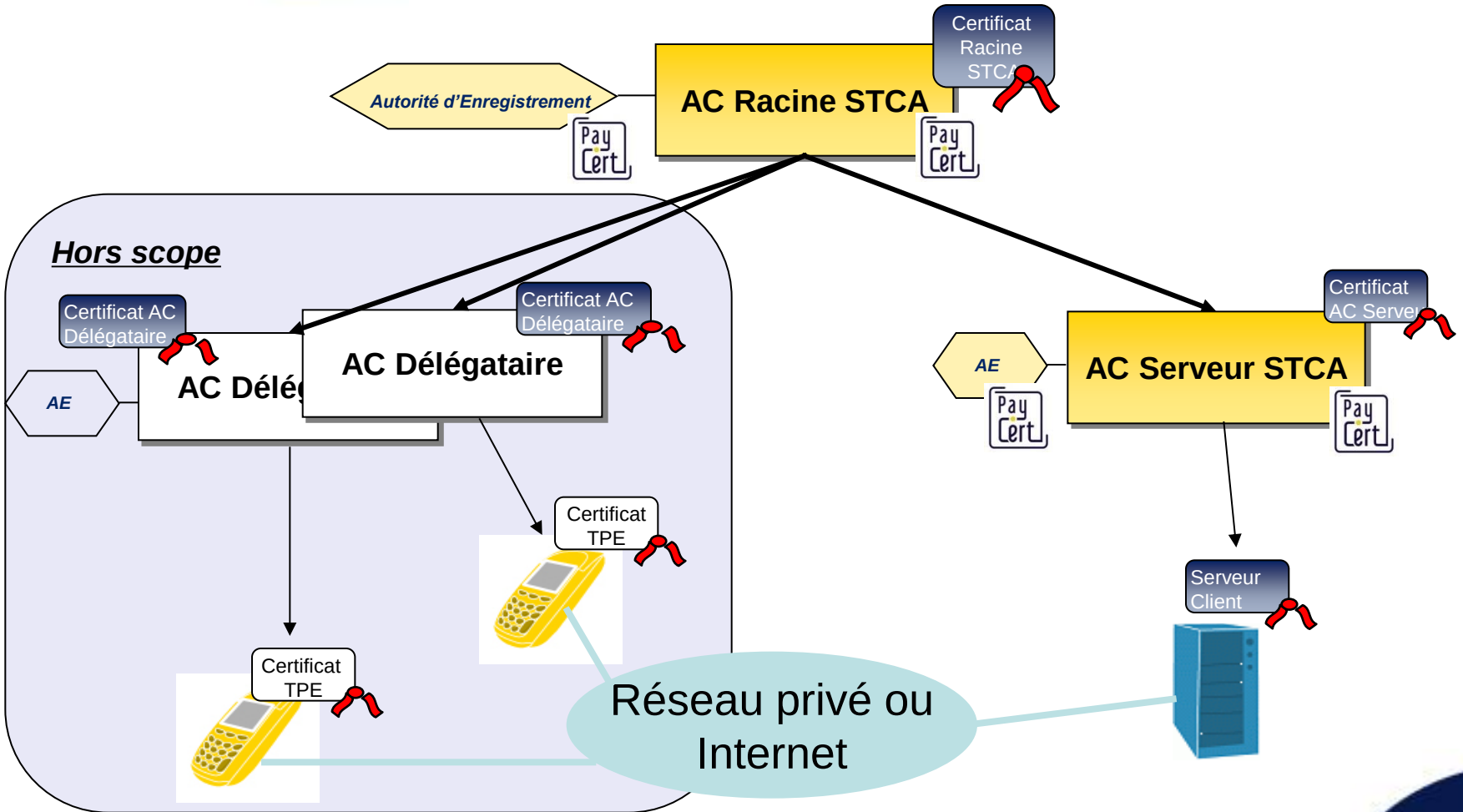
STCA : SHA-2

Ces modifications s'accompagneront d'une évolution tarifaire qui prendra effet dès le 1er Juillet 2016 et nous permettra de proposer durant la phase de transition des certificats SHA-1 et SHA-2. Cette tarification reposera sur le nombre de certificats demandés (par lot de 1 à 5 certificats), mais aussi sur le nombre d'AC sollicitées.

Désignation	Prix unitaire hors taxes
Certificats serveurs Sur une même AC : soit « Secure Transactions CA », soit « Secure Transactions CA - SHA2 » *(Lot de 1 à 5 certificats)*	3 330 Euros
Certificats complémentaires ▪ Utilisation d'une autre AC ▪ Utilisation d'un autre algorithme d'empreinte numérique (sur Secure Transactions CA) *(Lot de 1 à 5 certificats)*	1 250 Euros

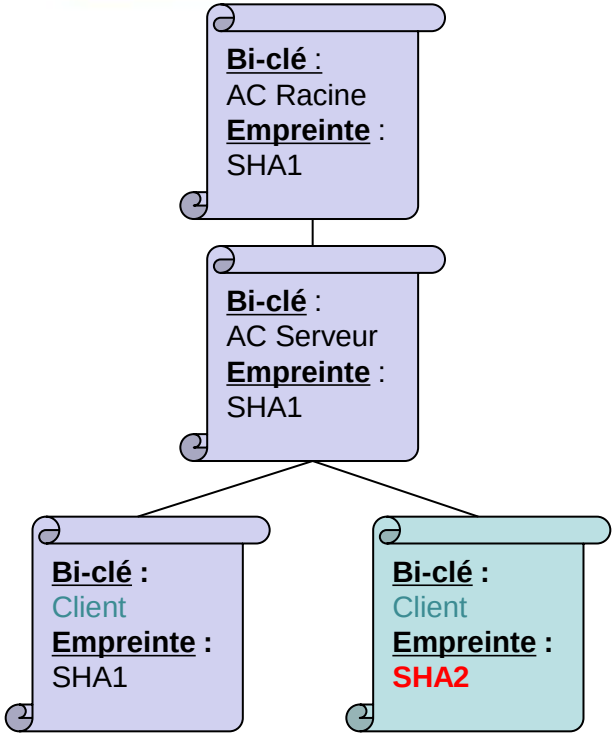
Vous trouverez dans ce document, une synthèse de la migration telle que prévue à ce jour, ainsi que des jalons prévisionnels. N'hésitez pas à nous remonter toutes remarques ou contraintes terrain que vous pourriez identifier et qui seraient de nature à impacter le processus prévu.

Architecture générale



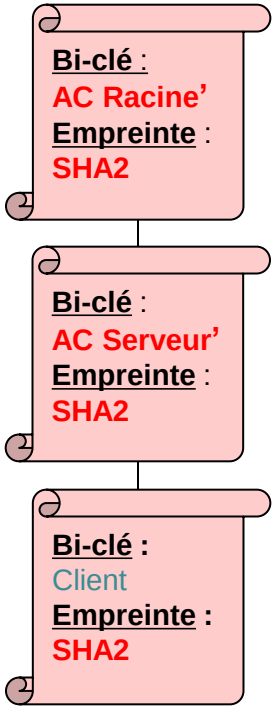
Connexion sécurisée

La migration



Secure Transactions CA

- Signatures possibles selon 2 options :
  - sha1WithRSAEncryption
  - sha256WithRSAEncryption
- Bi-clés : inchangés
- Fin de vie de la branche : inchangées
- Génération de certificats : jusqu'à 31/12/2018



Secure Transactions CA SHA-2

- Signatures : sha256WithRSAEncryption
- Bi-clés : nouveaux bi-clés

Les jalons

Type	*Révocation (branche existante)*	*Révocation (nouvelle branche)*
AC Racine	Inchangée	2046
AC Serveur	Inchangée	2036
Serveurs	2 ans	2 ans

Pour toute demande de renseignements, contactez :

Didier DUVILLE
didier-duville@paycert.eu
Tel : +33 1 40 15 59 34

STCA - Secure Transactions Certification Authority
PayCert
dossier.enregistrement@secure-transactions-ca.eu
Tel : +33 1 40 15 59 30