# Certificats racines utilisant un algorithme de hachage non sécurisé

ID METSYS : 7  
ID PingCastle : [A-WeakRSARootCert2](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html), [A-SHA1RootCert](https://pingcastle.com/PingCastleFiles/ad_hc_rules_list.html)  
ID ANSSI : [vuln3\_certificates\_vuln](https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#certificates_vuln)

Charge de travail : 3 jours  
Difficulté : 2 - Requière quelques connaissances sur l'infrastructure et l'anomalie qu'elle contient

****Description****

Certains algorithmes cryptographiques / longueurs de clés ne sont plus considérés comme sûr et doivent être abandonnés.

****Recommandation****

Remplacer ces certificats par de nouveaux utilisant des algorithmes plus récents et plus sûr (SHA2 / SHA256 et des clés plus longues).