rfc5937

Utilisation des contraintes d'ancre de confiance durant le traitement de chemin de certification

Ce document décris comment utiliser les informations utilisée avec une clé publique d'ancre de confiance lors de la validation de chemin de certification. Cette information peut être utilisée pour contraindre l'utilisation d'une ancre de confiance. Typiquement, les contraintes sont utilisées pour limiter les stratégies de certificat et les noms qui peuvent apparaître dans les chemins de certification validés en utilisant une ancre de confiance.

Les ancres de confiance sons largement utilisés pour vérifier les signatures numérique et la validation de chemin de certification (rfc5280). Il sont requis pour la validation de chemin de certification. La spécification du format de l'ancre de confiance (rfc5914) définis un moyen pour limiter le périmètre dans lequel une ancre de confiance peut être utilisée. La rfc5280 décris comment valider un chemin de certification. L'algorithme exige de traiter le nom et la clé depuis une ancre de confiance. L ?utilisation d'autres informations, incluant le renforcement de contraintes, est permis mais non requis, et le traitement des règles ne sont pas spécifiés.

Ce document définis un mécanisme pour identifier les contraintes qui devraient être forcés et les règles de traitement supplémentaires. Les règles supplémentaires spécifient une entrée additionnels et étendent les procédures d'initialisation dans l'algorithme de validation de chemin (rfc5280), les étapes de traitement post-initialisation ne sont pas affectés.

Identifier le contraintes d'ancre de confiance

TAF supporte 3 formats pour représenter les informations d'ancre de confiance : TrustAnchorInfor, Certificate, et TBSCertificate. Dans les 3 cas, les contraintes d'ancre de confiance peut être représentée comme extensions. Dans la structure TrustAnchorInfor, les stratégies de certificat, contraintes de stratégie, les contraintes de noms, inhibitAnyPolicy, et les contraintes de bases n'apparaîssent pas comme extensions et apparaîssent dans le champ CertPathControls.

Les extensions peuvent être marquées critique ou non. Quand les contraintes d'ancre de confiance sont forcées, les clients doivent rejeter les chemins de certification contenant une ancre de confiance avec des extensions critique non-reconnues. Quand les contraintes d'ancre de confiance ne sont pas forcées, les clients peuvent accepter les chemins de certification contenant une ancre de confiance avec les extensions critique non-reconnues. Les informations apparaissant dans le champ CertPathControls d'un objet TrustAnchorInfo doit être traité, pour s'assurer que les contraintes indiquées par ce champ sont forcés dans tous les cas.

Pour certains types de contrainte d'ancre de confiance, il y a un manque de concordance entre les paramètres pour l'algoritme de validation de chemin de certification et l'extension qui contient la contrainte. L'algorithme de validation de chemin de certification définis essentiellement l'initial-any-policy-inhibit, initial-policy-mapping-inhibit et initial-explicit-policy comme valeurs booléennes. les extensions inhibitAnyPolicy et policyConstraints qui correspondent à ces entrées sont exprimées en valeurs entières. Dans les étapes décrites ci-dessous, la présence de l'extension inhibitAnyPolicy résulte dans la valeur initial-any-policy-inhibit à TRUE. Si une extension policyConstraints est présente et contient un champ requireExplicitPolicy, la valeur initial-explicit-policy est à TRUE. Si une extension policyConstraints est présente et contient un champ inhibitPolicyMapping, la valeur initial-policy-mapping-inhibit est à TRUE.

Utiliser les contraintes durant le traitement de chemin de certification

Cet algorithme assume que les 9 entrées définies dans la rfc5280 sont fournis au traitement de chemin, plus une variable additionnelle :

enforceTrustAnchorConstraints Indique si les contraintes de l'ancre de confiance devraient être forcés

Les implémentations conformes ne sont pas obligés de supporter ce paramètre. Si une implémentation ne supporte pas le paramètre de ce flag, il doit valider tous les chemins de certification en utilisant une valeur de TRUE pour enforceTrustAnchorConstraints.

Initialisation

Si enforceTrustAnchorConstraints vaut false, aucune étape additionnelle n'est requise. Si enforceTrustAnchorConstraints vaut true, les étapes additionnelles suivante doivent être effectuées. Ces étapes (ou équivalentes) doivent être effectuées avant les étapes d'initialisation décrites dans la rfc5280.

- Si aucun nom distinct du sujet n'est associé avec l'ancre de confiance, la validation de chemin échoue. Le nom peut apparaître dans le champ subject d'un certification ou une structure TBSCertificate ou dans le champ taName de CertPathControls dans une structure TrustAnchorInfo.
- Si les contraintes de nom sont associées avec l'ancre de confiance, définis la variable initial-permitted-subtrees égale à l'intersection des permitted subtrees de l'ancre de confiance et de l'uinitial-permited-subtrees fournis par l'utilisateur. Si une de ces 2 entrées n'est pas fournie, la variable initial-permited-subtrees est définis à la valeur qui est disponible. Si aucun n'est fournis, la variable est définie à un jeu infinis.
- Si les contraintes de nom sont associées avec l'ancre de confiance, définis la variable initial-excluded-subtrees égal à l'union des excluded subtrees de l'ancre de confiance et de l'initial-excluded-subtrees fournis par l'utilisateur. Si une de ces 2 entrées n'est pas fournis, la variable est mis à la valeur qui est disponible. Si aucune n'est fournis, la variable est définie à un jeu vide.
- Si les stratégies de certificat sont associées avec l'ancre de confiance, définis la variable user-initial-policy-set égal à l'intersection des stratégies de certificat associés avec l'ancre de confiance et le user-initial-policy-set fournis par l'utilisateur. Si une de ces 2 entrées n'est pas fournie, la variable est définie à la valeur qui est disponible. Si aucune de ces valeurs n'est fournie, définis la variable à any-policy.
- Si une valeur inhibitAnyPolicy à TRUE est associée avec l'ancre de confiance (soit dans un CertPathControls, soit dans une extension inhibitAnyPolicy) et que la valeur initial-any-policy-inhibit vaut false, définis la valeur initial-any-policy-inhibit à true.
- Si une valeur de stratégie explicite requise est associée avec l'ancre de confiance (soit dans un CertPathControls, soit dans une extension policyConstraints) et que la valeur initial-explicite-policy vaut false, définis la valeur initial-explicit-policy à true.
- Si une valeur de mappage d'inhibition de stratégie est associée avec l'ancre de confiance (soit dans un CertPathControls, soit dans une extension PolicyConstraints) et que la valeur initial-policy-mapping-inhibit vaut false, définis la valeur initial-policy-mapping-inhibit à true.
- Si une extension de contrainte de base est associée avec l'ancre de confiance et contient une valeur pathLenConstraint, défins la variable d'état max_path_length égal à la valeur pathLenConstraint de l'extension de contrainte de base.

Traitement de certificat de base

Ce document n'exige pas d'augmentation d'étapes de traitement de certificat de base. Cepenadnt, certains types de contraintes d'ancre de confiance peuvent avoir définis des étapes additionnelles, par exemple, des contraintes de contenu CMS ou des contraintes de dédouanement de l'autorité.

Préparation pour le certificat i+1

Ce document ne nécessite aucune augmentation des étapes pour préparer le traitement du certificat i+1. Cependant, certains types de contraintes d'ancre de confiance peuvent avoir définies des étapes additionnelles, par exemple, des contraintes de contenu CMS ou des contraintes de dédouanement de l'autorité.

Procédure wrap-up

Ce document ne nécessite pas d'augmentation d'étapes de procédure d'enveloppement. Cependant, certains types de contraintes d'ancre de confiance peuvent avoir définies des étapes additionnelles, par exemple, des contraintes de contenu CMS ou des contraintes de dédouanement de l'autorité.

Relations à la rfc5280

Le traitement décris ci-dessous peut être incorporé dans une implémentation rfc5280 ou être implémenté comme pré-traitement aux entrées rfc5280 et post-traitement des sorties rfc5280.

Pour les contraintes de nom et les contraintes liées aux stratégies, le pré-traitement peut être utilisé, fournissant à l'implémentation rfc5280 la configuration des valeurs d'entrée user-initial-policy-set, initial-policy-mapping-inhibit, initial-explicit-policy, initial-any-policy-inhibit, initial-permitted-subtrees, et initial-excluded-subtrees. La rfc5280 ne définis pas d'entrée pour les contraintes de longueur de chemin, donc les contraintes de bases ne peuvent pas être implémentées en utilisant un pré-traitement. Il peut être implémenté comme post-traitement.

Certains types de contraintes d'ancre de confiance peuvent imposer des exigences additionnelles à l'implémentation rfc5280 pour supporter le pré-traitement et le post-traitement pour forcer les contraintes des ancres de confiance.

Considérations de sécurité

Les implémentations qui ne forcent par les contraintes d'ancre de confiance peuvent accepter certains chemins de certification rejetés par les implémentations qui imposent les contraintes d'ancre de confiance. Par exemple, une application qui ne force pas une contrainte de stratégie de certificat inclus dans une ancre de confiance peut accepter les certificats émis sous une stratégie de certificat qui fournis un niveau d'assurance plus faible que le niveau requis.

Les informations d'ancre de confiance doivent être stockées de manière sécurisée. Les changements d'information d'ancre de confiance peut impliquer l'acceptation de certificat qui devraient être rejetés. Par exemple, si une définition d'ancre de confiance est altérée pour supprimer une contrainte de noms, les applications peuvent accepter les certificats contenant les noms qui n'auraient été validés que dans des certificats validés par une ancre de confiance différente. Similairement, l'ajout d'ancres de confiance inapproprié à un dépôt d'ancre de confiance peut résulter en une validation de certificats via une ancre de confiance différente et avec des contraintes différente.

La rfc5914 et rfc5934 fournissent des considérations de sécurité additionnelles au regard de la préparation, le stockage, et l'utilisation d'ancres de confiance. La rfc5280 fournis des considérations de sécurité additionnelles au regard de l'utilisation des contraintes de nom.