



NORME INTERNATIONALE ISO/CEI 9594-3:1998
RECTIFICATIF TECHNIQUE 1

Publié 2002-03-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'annuaire: Définitions du service abstrait

RECTIFICATIF TECHNIQUE 1

Information technology — Open Systems Interconnection — The Directory: Abstract service definition

TECHNICAL CORRIGENDUM 1

iTeh STANDARD PREVIEW **(standards.iteh.ai)**

Le Rectificatif technique 1 à la Norme internationale ISO/CEI 9594-3:1998 a été élaboré par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 6, *Téléinformatique*.

<https://standards.iteh.ai/catalog/standards/sist/80960743-8571-412e-89ae-829ab598d9c1/iso-iec-9594-3-1998-cor-1-2002>

iTeh STANDARD PREVIEW **(standards.iteh.ai)**

ISO/IEC 9594-3:1998/Cor 1:2002

<https://standards.iteh.ai/catalog/standards/sist/80960743-8571-412e-89ae-829ab598d9c1/iso-iec-9594-3-1998-cor-1-2002>

NORME INTERNATIONALE
RECOMMANDATION UIT-T

TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DES SYSTÈMES
OUVERTS – L'ANNUAIRE: DÉFINITION DU SERVICE ABSTRAIT

CORRIGENDUM TECHNIQUE 1

1) Corrections du rapport d'erreurs 9594/166

Paragraphe 7.11.1.1 – Déréférencement d'un alias

Modifier l'avant-dernière phrase du premier paragraphe comme suit:

Si l'agent DSA transmet la requête à un autre agent DSA et reçoit un renvoi de référence de celui-ci en retour, les commandes d'accès doivent être appliquées au renvoi si l'objet cible targetObject qui y figure est le même que celui de la requête qui a fait l'objet du chaînage.

2) Corrections du rapport d'erreurs 9594/179

Annexe B, Figure B.4

Dans l'organigramme "**Retour de nom distinctif**", ajouter sous la question "**Alias disponible?/Non**" une question supplémentaire:

"Opération Read?"

donnant les réponses suivantes:

Oui: Erreur sur le nom

Non: passer à la question suivante: L'entrée correspond à l'objet (de base) de l'opération DAP?

Annexe B, Figure B.5

Dans l'organigramme "**Opération de lecture**", remplacer dans la partie droite le texte suivant de la dernière étape du traitement de l'expression "**ensemble selection vide = oui**"

"Retour de résultat de l'opération **Read**"

par

"Retour de résultat de l'opération **Read** ou de **nameError**".

3) Corrections du rapport d'erreurs 9594/188

Paragraphe 11.1.5 – Points de décision de l'opération d'adjonction pour le contrôle d'accès de base, alinéa 3)

Reformuler la NOTE 2 comme suit:

"La permission d'adjonction doit être fournie en tant qu'information de contrôle d'accès normative prescriptiveACI lors d'une tentative d'ajonction d'une entrée, ou en tant qu'information de contrôle d'accès normative prescriptiveACI, ou de sous-entrée subentryACI lors d'une tentative d'adjonction d'une sous-entrée".

4) Corrections du rapport d'erreurs 9594/202

Paragraphe 7.10 – Paramètres de sécurité

Remplacer le paragraphe décrivant l'itinéraire de certification **CertificationPath** par le texte suivant:

Le composant **CertificationPath** est une séquence contenant le certificat d'utilisateur du signataire et, en option, une séquence d'un ou de plusieurs certificats d'autorité de certification (CA) (voir article 8 de la Rec. UIT-T X.509 | ISO/CEI 9594-8). Le certificat d'utilisateur sert à lier la clé publique du signataire à son nom distinctif, et peut être utilisé pour vérifier la signature dans un argument de requête, dans une réponse ou dans une erreur. Ce paramètre doit être présent et doit contenir le certificat d'utilisateur du signataire si l'argument de requête, la réponse ou l'erreur est signé. Des certificats supplémentaires peuvent être présents et peuvent servir à déterminer si le certificat d'utilisateur du signataire est valable. Des certificats supplémentaires ne sont pas exigés si le destinataire dépend de la même autorité de certification que le signataire. Si le destinataire exige un itinéraire de certification pour validation, et qu'un paramètre susceptible d'être accepté n'est pas présent, la question de savoir si le destinataire refuse la signature ou tente d'établir l'itinéraire de certification relève d'une initiative locale.

Remplacer le paragraphe décrivant le temps **time** par le texte suivant:

Le paramètre **time** est le délai prévu de validité de la requête, de la réponse ou de l'erreur. Il est utilisé conjointement avec le nombre aléatoire pour permettre la détection d'attaques de type "réexécution".

Remplacer le premier paragraphe décrivant le paramètre aléatoire **random** par le texte suivant:

La valeur aléatoire **random** est un nombre qui doit être différent pour chaque requête, pour chaque réponse ou pour chaque erreur. Il est utilisé conjointement avec le paramètre **time** pour permettre la détection d'attaques de type "réexécution". Si l'intégrité de séquence est requise, l'argument aléatoire peut être utilisé pour acheminer un nombre d'intégrité de séquence comme suit: ...

5) Corrections du rapport d'erreurs 9594/206

Paragraphe 10.1.3 – Résultats de l'opération de listage

Dans l'avant-dernier paragraphe de la sous-section, modifier la première partie de la première phrase "Quand l'agent DUA a demandé une demande de protection de type signée, le paramètre **uncorrelatedListInfo** ..." comme suit:

"Quand l'agent DUA a demandé une demande de protection du type signée, ou quand l'annuaire n'est pas en mesure pour d'autres motifs de corréler les informations, le paramètre **uncorrelatedListInfo** ...".

6) Corrections du rapport d'erreurs 9594/217

Paragraphe 7.10 – Paramètres de sécurité

Remplacer la syntaxe du code d'opération **operationCode** dans les paramètres de sécurité **SecurityParameters** par la syntaxe suivante:

operationCode [6] Code OPTIONAL

Le **Code** doit être importé de:

Remote-Operations-Information-Objects

{joint-iso-ccitt remote-operations(4) informationObjects(5) version1(0)}

et, dans le paragraphe décrivant le code d'opération **operationCode**, supprimer les mots "identificateur d'objet". Remplacer aussi à la fin du même paragraphe les mots:

"ou aux résultats"

par les mots:

", aux résultats ou aux erreurs".

Ajouter à la syntaxe des paramètres de sécurité **SecurityParameters** le texte suivant:

errorCode [9] Code OPTIONAL

ainsi que la description suivante:

Le paramètre **errorCode** sert à rendre le code d'erreur sûr lorsqu'une erreur est renvoyée en réponse à une opération.

7) Corrections du rapport d'erreurs 9594/211

Paragraphe 7.10

Remplacer le paramètre **UTCTime** par **Time**:

Insérer le texte suivant après la définition en ASN.1 de la demande de protection **ProtectionRequest**:

```
Time ::= CHOICE {
    utcTime          UTCTime,
    generalizedTime  GeneralizedTime }
```

Insérer le texte suivant après le dernier paragraphe du paragraphe 7.10:

Si la syntaxe du paramètre **Time** a été choisie de manière à être du type **UTCTime**, la valeur du champ d'année à deux chiffres doit être rationalisée comme suit en une valeur d'année à quatre chiffres:

- si la valeur à 2 chiffres est comprise entre 00 et 49, inclusivement, il faut lui ajouter 2000;
- si la valeur à 2 chiffres est comprise entre 50 et 99, inclusivement, il faut lui ajouter 1900.

NOTE – Le temps généralisé **GeneralizedTime** doit être utilisé si la version négociée est la version **v2** ou une version ultérieure. Lorsque la version **v1** a été négociée, l'emploi du paramètre **GeneralizedTime** peut prévenir l'interfonctionnement avec des implémentations qui ne savent pas qu'elles ont le choix entre **UTCTime** et **GeneralizedTime**. Il incombe à ceux qui sont chargés de spécifier les domaines dans lesquels la présente spécification d'annuaire sera utilisée, par exemple les groupes de profilage, de déterminer quand le paramètre **GeneralizedTime** peut être utilisé. Le paramètre **UTCTime** ne sera en aucun cas employé pour indiquer des dates ultérieures à 2049.

Paragraphe 8.1.1

Remplacer dans le type en ASN.1 **SimpleCredentials** la valeur de la validité **validity** par le texte suivant:

```
Validity [1] SET {
    validityPeriod CHOICE {
        COMPONENTS OF ValidityPeriodUTC, -- UTC quand v1
        COMPONENTS OF ValidityPeriodGT, -- GT quand > v1
        random1 [2] BIT STRING OPTIONAL,
        random2 [3] BIT STRING OPTIONAL }
```

Insérer le texte suivant après le type en ASN.1 **SimpleCredentials**:

```
ValidityPeriodUTC ::= SET {
    time1 [0] UTCTime OPTIONAL,
    time2 [1] UTCTime OPTIONAL }
ValidityPeriodGT ::= SET {
    time1 [0] GeneralizedTime OPTIONAL,
    time2 [1] GeneralizedTime OPTIONAL }
```

Paragraphe 8.1.2

Insérer le texte suivant après le deuxième paragraphe:

NOTE – La période de validité **ValidityPeriodGT** doit être utilisée si la version négociée est la version **v2** ou une version ultérieure. Lorsque la version **v1** a été négociée, l'emploi du paramètre **ValidityPeriodGT** peut prévenir l'interfonctionnement avec des implémentations qui ne savent pas qu'elles ont le choix entre **ValidityPeriodUTC** et **ValidityPeriodGT**. Il incombe à ceux qui sont chargés de spécifier les domaines dans lesquels la présente apécification d'annuaire sera utilisée, par exemple les groupes de profilage, de déterminer quand le paramètre **ValidityPeriodGT** peut être utilisé. Le paramètre **ValidityPeriodUTC** ne sera en aucun cas employé pour indiquer des dates ultérieures à 2049.

Remplacer dans le type en ASN.1 **Token** la valeur du paramètre **time** par le texte suivant:

```
time [2] Time
```

Apporter également les modifications à l'ASN.1 de l'Annexe A.