

# Upgrade-Checkliste für Expressway 15.5.20

## Inhalt

---

[Einleitung](#)

[Verwendete Komponenten](#)

[Vor dem Upgrade](#)

[Lesen des Zertifikats](#)

[Vorgehensweise vor dem Wartungsfenster](#)

[Wenn das Upgrade fehlschlägt](#)

[Die Bereitschaftsprüfung hat das Upgrade gestoppt](#)

[Alarm nach dem Hochfahren eines Knotens](#)

[Administrator kann sich nicht anmelden](#)

[Fehler bei Zertifikat oder Peer-Identität](#)

[Cluster-Alarm während oder nach dem Upgrade](#)

[Probleme bei der Anmeldung nach dem Hochfahren des Knotens](#)

[Sammelbelege für den Fall, dass ein TAC-Fall erforderlich ist](#)

[Nach dem Upgrade](#)

[Auf jedem Knoten](#)

[Nur Cluster](#)

[Service-Prüfungen nach verwendetem System](#)

---

## Einleitung

In diesem Dokument wird beschrieben, wie Sie Expressway für das X15.5.20-Upgrade zur Erhöhung der Sicherheit vorbereiten. Es listet alle Voraussetzungen auf und zeigt, wie sie behoben werden können.

## Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

### Vor dem Upgrade

---



Vorsicht: Starten Sie erst dann ein Cluster-Upgrade, wenn jeder Peer die Bereitschaftsprüfungen bestanden hat. Legen Sie die TLS-Verifizierung auf Erzwingen fest, und bestätigen Sie, dass der Cluster fehlerfrei ist. Verwenden Sie ein Peer-Identitätsformat, keine Kombination aus IP-Adressen und FQDNs. Jedes Serverzertifikat

---

muss den FQDN dieses Knotens im SAN oder nur dann im CN enthalten, wenn das SAN leer ist. Ein leeres SAN kann auftreten, wenn OpenSSL zur Erstellung des CSR verwendet wurde. Wenn eine Überprüfung fehlschlägt, wird das Upgrade beendet, ohne die vorhandene Clusterkonfiguration zu ändern.

| Überprüfen                                                                                  | Standalone                                               | Cluster                                                                                  | Wenn es nicht wahr ist                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------|----------------------------------------------------------|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Upgrade-Pfad entspricht <a href="#">Anhang 3</a>                                            | Erforderlich                                             | Erforderlich                                                                             | Stoppen Sie vor X8.11.4 zuerst bei X8.11.4. Konvertieren der X12 PAK-Lizenzierung in <a href="#">Smart Licensing vor X15.x</a> .                                                                                                         |
| Aktuelles Backup und getesteter Rollback-Plan                                               | Erforderlich                                             | Auf jedem Knoten erforderlich                                                            | Nehmen Sie die Sicherung vor dem Fenster. Ein späteres Zurücksetzen auf die Werkseinstellungen löscht die Konfiguration.                                                                                                                 |
| Cluster ist fehlerfrei, keine ungeklärten Alarme, Replikation ist synchronisiert            | Nicht zutreffend                                         | Erforderlich                                                                             | Reparieren Sie den Cluster vor dem Upgrade. Bei einem rollierenden Upgrade wird weiterhin das normale Split-Cluster-Verhalten verwendet.                                                                                                 |
| <a href="#">Die TLS-Verifizierung wird durchgesetzt</a> , und der Cluster ist fehlerfrei.   | Nicht zutreffend                                         | Vor dem Upgrade erforderlich                                                             | Ändern Sie "Permissive" in "Enforcing" (Erzwingen), korrigieren Sie das Zertifikat, und bestätigen Sie die Replikation. Erkennen Sie dies nicht im Fenster.                                                                              |
| Jeder Peer verwendet dasselbe Identitätsformat, und die Peerliste ist nicht leer.           | Peer-Identitätsprüfung besteht                           | Erforderlich. Gemischte IP- und FQDN-Adressen werden vor dem Neustart blockiert          | Standardisierung aller FQDNs oder IP-Adressen, Replikation der Änderungen und Überprüfung der Integrität des Clusters Ändern Sie das Format nicht während eines rollierenden Upgrades.                                                   |
| Serverzertifikat enthält den System-FQDN im SAN oder im CN nur, wenn das SAN leer ist       | Erforderlich, wenn das Upgrade das Zertifikat überprüft. | Erforderlich. Das Upgrade wird beendet und die Cluster-Konfiguration bleibt unverändert. | Geben Sie das Zertifikat erneut ein. Wenn ein SAN vorhanden ist, verlassen Sie sich nicht auf den CN. Ablehnen von Namen, die eine eingebettete NUL enthalten.                                                                           |
| Zertifikat ist datiert, vertrauenswürdig durch Peers, RSA 2048+ oder P-256+, SHA-2-Signatur | Empfohlen                                                | Erforderlich                                                                             | <a href="#">SHA-1-Signaturen werden von X15.2 bereits nicht unterstützt</a> . Geben Sie das Zertifikat erneut ein. Ein selbstsigniertes Zertifikat ist nur zulässig, wenn jeder Peer explizit so konfiguriert ist, dass er ihm vertraut. |
| TCP 4371 nur von                                                                            | Empfohlen                                                | Erforderlich                                                                             | Einschränkung der Firewall Dies ist                                                                                                                                                                                                      |

| Überprüfen                                                                                        | Standalone                               | Cluster                                  | Wenn es nicht wahr ist                                                                                                                               |
|---------------------------------------------------------------------------------------------------|------------------------------------------|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| bekannten Peers zulässig                                                                          |                                          |                                          | eine umfassende Abwehr für ClusterDB. Es ist kein Ersatz für das Upgrade.                                                                            |
| Prüfung von Admin-API-Clients                                                                     | Erforderlich, wenn APIs verwendet werden | Erforderlich, wenn APIs verwendet werden | Erwarten Sie eine strengere Überprüfung von Namen und Passwörtern, CSRF-Prüfungen bei FormPutXML-Schreibvorgängen und keine optionale Schlüssel-API. |
| Das Wartungsfenster deckt ein rollierendes Upgrade sowie einen möglichen kurzen Cluster-Alarm ab. | Normales Fenster                         | Erforderlich                             | Die erneute Cookie-Verschlüsselung kann eine Clusterkommunikationswarnung auslösen. Es wird erwartet, dass sie von selbst abgebaut wird.             |

## Lesen des Zertifikats

Exportieren Sie das Serverzertifikat, und überprüfen Sie es.

- FQDN im SAN. Die [Versionshinweise](#) erfordern den System-FQDN in einem SAN. Die CN wird nur aktiviert, wenn die SAN-Erweiterung leer ist.
- Kein CN-Fallback. Wenn ein SAN vorhanden ist und nicht übereinstimmt, [schlägt die Überprüfung auch dann fehl, wenn die CN korrekt ist](#). Geben Sie alle erforderlichen DNS-Namen oder IP-Adressen in den richtigen SAN-Typ ein.
- NUL-Zeichen. Ein Zertifikatsname, der eine eingebettete NUL enthält, wird abgelehnt.
- Termine `notBefore` muss in der Vergangenheit liegen und `notAfter` muss in der Zukunft liegen.
- Wichtigste. RSA mindestens 2048 Bit, oder ein EC-Schlüssel auf P-256 oder höher.
- Unterschrift. SHA-2-Familie. Ab X15.2 werden [sha1WithRSAEncryption und ecdsa-with-SHA1](#) nicht unterstützt.
- Aussteller. Wenn Betreff und Aussteller identisch sind, erfolgt die Selbstsignierung. Peers müssen ihr bereits vertrauen.

## Vorgehensweise vor dem Wartungsfenster

- Legen Sie vor dem Fenster die TLS-Überprüfung des Clusters auf [Erzwingen fest](#), starten Sie den Cluster neu (beginnend mit dem Publisher), und bestätigen Sie, dass der Cluster fehlerfrei ist. Der permissive Modus wird nicht unterstützt. Ein älterer Permissive-Wert kann sichtbar bleiben, umgeht jedoch nicht die ClusterDB-Zertifikatvertrauensstellung oder die Überprüfung der Peer-Identität.
- Bei den Peer-Identitäten muss es sich entweder um FQDNs oder um IP-Adressen handeln. Ändern Sie dieses Format nicht, während ein Rolling Upgrade ausgeführt wird.
- Ein authentifizierter H.323-Endpunkt mit mehr als einem Alias kann für jeden Alias eine [Aliaszuordnung](#) für Anmeldeinformationen benötigen, oder die Aliasbindung für

Anmeldeinformationen in der Unterzone ist deaktiviert. Das Deaktivieren der Bindung schwächt den Sicherheitsstatus.

- Das Ablaufdatum des lokalen Admin-Kennworts bleibt deaktiviert, wenn PasswordExpiryDays den Wert 0 hat. Wenn es aktiviert ist, wird das Ablaufdatum um 00:00 UTC und nicht um Mitternacht berechnet.
- [Die Kennwortverlaufstiefe beträgt standardmäßig 12](#). Der Trainingsbereich liegt zwischen 3 und 24. Leere Administratorkennwörter werden abgelehnt, und ein kürzlich verwendetes Kennwort kann abgelehnt werden.
- [Für die LDAP-Administrator-Rollenzuordnung](#) ist eine exakte Übereinstimmung mit dem Gruppennamen erforderlich. Ein Gruppenname, der nur den konfigurierten Namen enthält, gewährt die Rolle nicht mehr.
- Bei einer neuen Installation, einem Zurücksetzen auf die Werkseinstellungen oder einer unbeaufsichtigten Bereitstellung kann ein [werkseitig voreingestelltes Root-Kennwort nicht wiederverwendet werden](#). Bei einer Aktualisierung wird das aktuelle Administratorkennwort nicht gelöscht.
- Ein schreibgeschützter Administrator kann die SAML IdP-Vertrauensstellung nicht mehr ändern.
- E-Mail, die STARTTLS nicht abschließen kann, wird nicht unverschlüsselt gesendet.
- [Smart Licensing](#) ist der einzige Lizenzierungsmodus. Die PAK-Optionsschlüssel wurden in X14.2 entfernt. Das Standard-Expressway-Image ermöglicht [2.500 verschlüsselte Signalisierungssitzungen](#). Expressway Select ist das nicht abgedeckte Bild.

## Wenn das Upgrade fehlschlägt

Lassen Sie den Cluster so, wie er ist. Eine fehlgeschlagene Bereitschaftsprüfung ändert die vorhandene Clusterkonfiguration nicht. Setzen Sie einen Knoten nicht auf die Werkseinstellungen zurück, um den Fehler zu überwinden.

### Die Bereitschaftsprüfung hat das Upgrade gestoppt

Das Installationsprogramm wird vor dem Neustart beendet, wenn das Zertifikat, die TLS-Verifizierung oder die Peer-Identitätsanforderung fehlschlagen. Eigenständige Knoten bestehen die Peer-Identitätsprüfung.

### Alarm nach dem Hochfahren eines Knotens

Bei einem Burst der Neuverschlüsselung der Cluster-Datenbank kann es zu einem Alarm wegen eines Fehlers bei der Cluster-Kommunikation kommen. Gib ihm Zeit, fertig zu werden. Eskalieren Sie, wenn sie nicht abreißt.

### Administrator kann sich nicht anmelden

Behandeln Sie dies separat von einem Installationsfehler. Abgelaufene, wiederverwendete oder bei der ersten Anmeldung verwendete Kennwörter blockieren die Sitzung. Sie bedeuten nicht,

dass das Bild fehlschlug.

## Fehler bei Zertifikat oder Peer-Identität

1. Laden Sie einen vollständigen System-Snapshot von dem Knoten herunter, der gestoppt wurde. Öffnen Sie install-error im tmp-Verzeichnis dieses Snapshots.
2. Wenn es sich um die Peer-Identität handelt, überprüfen Sie, ob eine Kombination aus IP-Adressen und FQDNs vorhanden ist oder ob eine leere Peer-Liste vorhanden ist. Verwenden Sie für jeden Peer ein einziges Format, warten Sie auf die Replikation, bestätigen Sie, dass der Cluster fehlerfrei ist, und wiederholen Sie den Vorgang. Ändern Sie nicht das Identitätsformat während eines rollierenden Upgrades.
3. Wenn sich die Nachricht auf das Zertifikat bezieht, vergleichen Sie es mit der Regel für die Versionshinweise: Der System-FQDN muss sich im SAN befinden oder nur dann im CN, wenn das SAN leer ist. Ein vorhandenes SAN darf nicht auf den CN zurückgreifen.
4. Erneutes Ausstellen des Zertifikats mit allen erforderlichen DNS-Namen oder IP-Adressen im richtigen SAN-Typ. Ablehnen eines Namens, der eine eingebettete NUL enthält.
5. Vergewissern Sie sich, dass das neue Zertifikat das aktuelle vertrauenswürdige RSA 2048+ oder P-256+ ist und mit SHA-2 signiert wurde. Hängen Sie den privaten Schlüssel nicht an das Ticket an.
6. Legen Sie die TLS-Verifizierung auf Erzwingen fest, überprüfen Sie, ob der Cluster fehlerfrei ist, und wiederholen Sie den Upgrade auf dem Knoten, der gestoppt wurde.
7. Setzen Sie das Rolling-Upgrade erst fort, wenn der betreffende Knoten fehlerfrei ist. Aktualisieren Sie die verbleibenden Knoten nicht, während bei dieser Überprüfung ein Knoten angehalten wird.

## Cluster-Alarm während oder nach dem Upgrade

1. Bestätigen Sie, dass das Upgrade abgeschlossen ist und der Knoten X15.5.20 verwendet.
2. Suchen Sie im Ereignisprotokoll nach developer.upgrade-Meldungen über die Neuverschlüsselung von ClusterDB-Feldern, und klicken Sie dann auf "Migrierte Daten in CDB speichern".
3. Warten Sie, bis der Alarm gelöscht wird. Im Schulungsmaterial steht, dass die Verschlüsselung nach Abschluss der Neuverschlüsselung gelöscht wird.
4. Wenn sie erhalten bleibt, erfassen Sie den Cluster-Status, Alarme und einen Snapshot von jedem Peer. Kopieren Sie keine Cluster-Cookies oder Schlüsselmaterial in die Ticketnotizen.
5. Vergewissern Sie sich, dass TCP 4371 und 4372 nur zwischen den Peers geöffnet sind und das gegenseitige TLS erfolgreich ist. Eine Firewall, die 4371 von überall aus unterstützt, ist nicht die Lösung.

## Probleme bei der Anmeldung nach dem Hochfahren des Knotens

- Die Webbenutzeroberfläche leitet zu einer Kennwortänderung um. Das aktuelle Kennwort muss eingegeben werden, und das neue Kennwort muss anders sein. Dies wird bei der ersten GUI-Anmeldung nach einer Installation oder einem Zurücksetzen auf die Werkseinstellungen sowie nach Ablauf eines lokalen Kennworts erwartet.
- SSH sagt, dass "keyboard-interactive/PAM" fehlgeschlagen ist und niemals eine Shell öffnet.

Ein abgelaufenes lokales Kennwort muss geändert werden. Die alte Sitzung wird nicht gewährt.

- REST ergibt 401. Für einen abgelaufenen lokalen Administrator wird erwartet. Das Ereignisprotokoll kann Kennwortkonflikte oder TAA-chkpasswd-Fehler für den API-Bereich anzeigen. Ändern Sie das Kennwort, und wiederholen Sie den Vorgang.
- Neues Kennwort abgelehnt. Sie befinden sich im Verlauf (Standardwert letzte 12), oder die aktuellen Komplexitätsregeln wurden nicht eingehalten.
- Der LDAP-Administrator hat die erwartete Rolle verloren. Vergleichen Sie die konfigurierte Gruppe mit dem genauen Gruppennamen, der von LDAP zurückgegeben wurde. Ein Teil- oder Teilzeichenfolgenentsprechung gewährt die Rolle nicht mehr. Ein schreibgeschützter Administrator kann die SAML-IdP-Vertrauensstellung nicht bearbeiten.
- Bei einer neuen Installation oder einem Zurücksetzen auf die Werkseinstellungen ist kein Root-Kennwort vorhanden. Suchen Sie nicht nach Standardanmeldeinformationen, und geben Sie diese nicht weiter. Bei einem Upgrade wird das aktuelle Administratorkennwort nicht gelöscht.



Vorsicht: Das Zurücksetzen auf die Werkseinstellungen ist nicht der Upgrade-Wiederherstellungsschritt. Er löscht Cluster-Identitäts- und Cluster-Cookies. Ein vom System ausgelöstes Zurücksetzen nach der Entclustering oder eine inkonsistente Cluster-Datenbank behält die IP-Adresse sowie die Admin- und Root-Passwörter bei, löscht andere Konfigurationen und Protokolle und setzt den Knoten auf sein temporäres Zertifikat zurück. Verwenden Sie sie nur, wenn sie in den Versionshinweisen verlangt wird, und nur, wenn eine Sicherung vorhanden ist.

---

## Sammelbelege für den Fall, dass ein TAC-Fall erforderlich ist

1. Softwareversion und -rolle jedes Knotens sowie der Knoten, der gestoppt wurde.
2. Vollständiger System-Snapshot vom ausgefallenen Knoten, einschließlich tmp/install-error.
3. Serverzertifikattext (openssl x509 -text -noout). Kein privater Schlüssel.
4. Clusterstatus, Alarme und ob "xConfiguration Cluster TlsVerify" "Permissive" oder "Enforce" anzeigt.
5. Ereignisprotokollzeilen für das Upgrade und ggf. Fehler bei der sshd- oder httpd-Authentifizierung. Passwörter und Cookies korrigieren.
6. Unabhängig davon, ob lokale, LDAP- oder SAML-Administratoren, Smart Licensing oder eine beliebige API-Automatisierung verwendet wird.

## Nach dem Upgrade

### Auf jedem Knoten

1. Die Version ist der beabsichtigte X15.5.20-Build.
2. Der Knoten ist über seine Verwaltungsadresse erreichbar, und die Webbenutzeroberfläche wird geladen.

3. Es wird kein Alarm für neue Hardware, Festplatte oder Anwendung mehr ausgelöst.  
(Cluster-Kommunikationsalarm wird nach der Neuverschlüsselung gelöscht.)
4. Eine neue Sicherung wird durchgeführt, wenn der Cluster stabil ist.

## Nur Cluster

1. Jeder Peer ist aktiv, im Cluster, und die Replikation funktioniert einwandfrei.
2. Peers kommunizieren mit gegenseitigem TLS über TCP 4371 und 4372. (Eine Verbindung ohne gültiges Clientzertifikat muss fehlschlagen.)
3. Cluster-TlsVerify wird durchgesetzt.

Permissive wird nicht unterstützt. Ein Legacy-Permissive-Wert könnte weiterhin angezeigt werden, umgeht jedoch nicht die Validierung. Aktivieren Sie Durchsetzen, und stellen Sie sicher, dass der Cluster fehlerfrei bleibt.

4. Die Firewall lässt TCP 4371 weiterhin nur von den Peer-Adressen zu.
5. In den Protokollen oder den von Ihnen hochgeladenen Snapshot-Notizen wird kein Cluster-Cookie oder Diagnoseconsequence angezeigt.

## Service-Prüfungen nach verwendetem System

| Wenn                                 | Wie gut aussieht                                                                                                                                  | Wenn sie fehlschlägt                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lokale Administratoren               | GUI, SSH und API akzeptieren das aktuelle Kennwort.<br>Abgelaufene Konten werden zu einer Kennwortänderung weitergeleitet oder erhalten HTTP 401. | Vergewissern Sie sich, dass das Kennwort um 00:00 UTC abgelaufen ist und sich das neue Kennwort außerhalb des Verlaufs Fensters befindet.                                                                                                                                                                                                                                                                 |
| LDAP-Administratoren                 | Ein Administrator meldet sich nur an, wenn der LDAP-Gruppenname genau mit der konfigurierten Gruppe übereinstimmt.                                | Vergleichen Sie die Verzeichnisgruppe mit der Expressway-Gruppe. Erweitern Sie die Übereinstimmung nicht, um eine Anmeldung zu erzwingen.                                                                                                                                                                                                                                                                 |
| SIP- oder B2B-Anrufe                 | Ein Testanruf wird in beide Richtungen verbunden.                                                                                                 | Sammeln Sie den Anrufsverlauf und einen Snapshot.                                                                                                                                                                                                                                                                                                                                                         |
| Authentifizierte H.323-Registrierung | Der Endpunkt wird bei jedem verwendeten Alias registriert, einschließlich einer H.323-ID und einer E.164-Nummer.                                  | Fügen Sie für jeden Alias eine Aliaszuordnung mit Anmeldeinformationen hinzu. In den <a href="#">Versionshinweisen</a> wird xConfiguration Registration CredentialAliasMap mit dem Mustertyp Exact verwendet. Wenn Sie CredentialAliasBinding für die Unterzone deaktivieren, wird auch die Registrierung wiederhergestellt, und der Sicherheitsstatus wird geschwächt. H.323 selbst wird nicht entfernt. |

| Wenn                            | Wie gut aussieht                                                                                                                                                                                                       | Wenn sie fehlschlägt                                                                                                                                                                                                                                                                           |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MRA oder Device-Registrierung   | Ein bekannter Endpunkt registriert einen Anruf und führt ihn aus. SANs mit UC-Client-Zertifikat sind bestimmte DNS-Namen oder IP-Adressen und keine übermäßig breiten oder falsch formatierten Werte.                  | Vergleichen Sie Zertifikate, Traversal-Anmeldedaten und DNS mit dem Backup vor dem Upgrade. Erneutes Ausstellen eines Zertifikats, dessen SAN zu breit ist                                                                                                                                     |
| E-Mail-Benachrichtigungen       | Eine Testnachricht verlässt den Knoten mithilfe von STARTTLS.                                                                                                                                                          | Wenn STARTTLS nicht abgeschlossen werden kann, schlägt die Zustellung fehl geschlossen. Korrigieren Sie die Vertrauensstellung des Mailservers oder TLS. Erwarten Sie keinen Klartext-Fallback.                                                                                                |
| Smart Licensing                 | Registrierung und Autorisierung entsprechen der Webbenutzeroberfläche. Das Standard-Image bleibt innerhalb von <a href="#">2.500 verschlüsselten Signalisierungssitzungen</a> , oder der Knoten ist Expressway Select. | Überprüfen Sie den Transport und CSSM. Das CSSM-Kontrollkästchen "exportgesteuerte Funktionalität zulassen" gilt nicht für Expressway. Durch das Aufheben des Tokens und das Löschen der Produktinstanz wird der Knoten auf Deregistered festgelegt. Optionstasten sind keine Problemumgehung. |
| REST oder Konfigurationsskripte | Kontonamen entsprechen der neuen Längen- und Zeichenbegrenzung. Konfigurationsschreibvorgänge beinhalten den von der GUI verwendeten CSRF-Schutz.                                                                      | Aktualisieren Sie den Client anhand des API-Schemas für den Versand. Ein entfernter/bereitstellender/optionkey-Aufruf wird voraussichtlich fehlschlagen.                                                                                                                                       |

### Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.