
# Sicherheitskonzept für

# Registration Authorities (RA)

zur Ausgabe des qualifizierten Zertifikats

# a.sign premium

Version 2.1.2

INHALT



Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

# Grundlagen

Die erforderliche Sicherheit der Zertifizierungsdienste wird durch ihre planmäßige Dokumentation transparent und überprüfbar gemacht.

- Bedrohungs- und Risikoanalyse,
- Sicherheitskonzept und
- Betriebskonzept

der a.trust begründen die jeweils zu treffenden Sicherheitsmaßnahmen, deren Einhaltung mittels Audits laufend zu kontrollieren ist (Revision).

**Aus dem Gesamtsicherheitskonzept sind in folgenden Inhaltsbereichen Maßnahmen für den Zertifizierungsdienst Registrierung abzuleiten:**

# 1. Vertragsverhältnis a.trust – RA (RA-Vertrag)

Eine RA kann nur auf Basis eines mit a.trust geschlossenen Vertrages aktiv sein (Autorisierte Registrierungsstellen). Das Vertragsverhältnis schließt Regelungen zur Softwarenutzung durch die RA mit ein.

# 2. Personal der RA

Die Zuverlässigkeit von Mitarbeitern, die in einer RA und im Namen der a.trust mit Registrierungsaufgaben (Registration Officer = RO) betraut sind, wird prinzipiell anhand eines alle zwei Jahre vorgelegten Auszugs aus dem Strafregister nachgewiesen. Bei Bankmitarbeitern geht die a.trust von der Erfüllung dieser Kriterien und deren interner Kontrolle aus, womit bei Banken als RA die Vorlage des Strafregisterauszugs der Mitarbeiter entfallen kann.

Mit Registrierungsaufgaben betraute Mitarbeiter einer RA erfüllen ihre Aufgaben als RO oder zRO (zentraler RO). RO und zRO erhalten die für ihre Tätigkeiten erforderliche Qualifikation in speziellen von a.trust selbst oder von a.trust dazu autorisierten Ausbildungspartnern angebotenen Schulungen. Die RA kann dann ihre RO intern ausbilden, wenn sie über von a.trust geschulte interne Trainer verfügt oder autorisierte externe Trainer beauftragt. Trainer und zRO werden direkt von a.trust ausgebildet. Nur ausgebildete Mitarbeiter erhalten die zur Durchführung ihrer Tätigkeiten notwendige RO-Berechtigung.

Als dessen Hotline muss für den RO innerhalb der RA immer ein zRO erreichbar sein.

# 3. Infrastruktur

- Lage des Aufbewahrungsraumes für Signaturkarten
- Lage des Aufbewahrungsraumes für Dokumente/Datenträger

(Siehe dazu auch Anhang I: „Anforderungen an den RO-Arbeitsplatz“)



# 4. Hardware

- Schutz des Bildschirms und der Tastatur, bzw. der Kartenleser des Arbeitsplatzes vor Einsichtnahme durch Unberechtigte
- Schutz des Druckers des RO-Arbeitsplatzes vor Einsichtnahme durch Unberechtigte
- Schutz des Scanners des RO-Arbeitsplatzes vor Einsichtnahme durch Unberechtigte

(Siehe dazu auch Anhang I: „Anforderungen an den RO-Arbeitsplatz“)

# 5. Paperware

- Genaue Überprüfung des Lichtbildausweises
- Im Zweifelsfall keine Ausgabe der Signaturkarte an den Antragsteller. Diesem wird empfohlen, mit einem überprüfbaren Ausweis wieder zu kommen
- Die Mitarbeiter der RA werden auf die Überprüfung der Ausweise geschult
- (Einscannen und) Elektronische Archivierung des Ausweises, um einen späteren Nachweis erbringen zu können
- Identifikation des Antragstellers mit Lichtbildausweis bei jeder Datenänderung, Passwortauskunft, etc.
- Einscannen und elektronisches Archivieren des unterschriebenen Antragstellerformulars
- Ausdruck des Antragstellerformulars in der RA
- Der Antragsteller bestätigt mit Unterschrift, dass er die Belehrung gemäß SigG/SigV erhalten hat
- Kontrolle des Antragstellerformulars/der erhobenen Daten mit dem Signator
- Ausgedruckte PIN hat nur die Funktion einer Initial-PIN, mit der nicht signiert werden kann
- Änderung der Initial-PIN in der RA anlässlich der Kartenabholung
- Zertifikat wird im Beisein des Antragstellers ausgestellt, auf die Karte gespeichert und mit Zustimmung des Antragstellers im Directory Service veröffentlicht

# 6. Software

- Durchführung von Registrierungstätigkeiten nur mit berechtigter RO-Karte
- Übermittlung von Bestelldaten muss mit der RO-Karte signiert sein
- Zwingende Eingaben in der RA-Software
- Prüfung der Bestellung in der RA-Software mit Änderung/Ablehnung im Fehlerfall
- Ausstattung des Bestellsystems mit Hilfefunktionen
- Ausstattung des RO mit RO-Handbuch
- Durchlauf des Schulungsprogramms für ROs



# 7. Datenträger

- Meldung des Verlustes einer noch nicht ausgegebenen Bestellkarte: RO an zRO an die a.trust mit Dokumentation der Verlustmeldung
- Übernahmebestätigung der RA an das Transportunternehmen bezüglich der vollständigen Lieferung von Bestellkarten
- Kartenlagerung der Bestellkarte im Tresor der RA
- Die RA ist für die Schulung der autorisierten Personen verantwortlich und haftet für die Schäden, die aus der Missachtung dieser Verantwortung entstehen
- Bei Defekt oder falscher Beschriftung muss die Bestellkarte sicher vernichtet und eine Ersatzbestellung veranlasst werden
- Antragsteller bestätigt die Übernahme der unbeschädigten Signaturkarte
- Stichprobenhafte Inventur der Signaturkarten durch Verantwortlichen in der RA
- Stornierung und sichere Vernichtung nicht abgeholter Signaturkarten nach 3 Monaten. Die Veranlassung der Stornierung muss dokumentiert werden
- Zusenden der Bestellkarte an die ausgebende RA-GS
- Transportprotokolle der Bestellkarte werden mit der Bestellkarte gelagert und ausgegebene Bestellkarten auf dem Transportprotokoll vermerkt

# 8. Anwendungsdaten

- Schutz des Bildschirms und der Kartenlesegeräte des RO-Arbeitsplatzes vor Einsichtnahme durch Unberechtigte
- Schutz von Drucker und Scanner des RO-Arbeitsplatzes vor Einsichtnahme durch Unberechtigte
- Identifikation des Antragstellers mittels Ausweiskontrolle bei jeder Antragstellung

# 9. Kommunikation

- SSL Verbindung zwischen RO-PC und Rechenzentrum der a.trust
- Signatur der Anträge mit der RO-Karte
- Signatur von Änderungen im Bestellsystem mit der RO-Karte
- Sofortiger Abbruch der sicheren Verbindung bei Entfernen der RO-Karte

# 10. Audit (Revision)

Mit der Kontrolle der Umsetzung der Sicherheitsmaßnahmen (Revision) befasste Stellen:

- Interne Revision der jeweiligen RA
- a.trust
- RTR GmbH (TKK)

Die RA muss a.trust den für intern organisierte Audits Verantwortlichen nennen.

Audits haben jedenfalls folgende Punkte zu beinhalten:

- Technische Ausstattung des RO-Arbeitsplatzes
- Überprüfung der RO auf Schulungsteilnahme
- Aufliegen der aktuellen Dokumente: „RA-Ordner“
- Archivierung des Antragstellerformulars
- Sichere Kartenlagerung
- Kontrolle des Kartenbestands anhand der alten Produktionsprotokolle (Lieferschein)
- Möglichkeit der Änderung einer Signatur-PIN ohne Einsicht eines Mitarbeiters oder eines anderen Kunden
- Vernichten von Karten
- Kontrolle der archivierten Identifikationsdaten (bei a.trust)

(Zur Durchführung von Audits in der Praxis siehe Anhang III: „Audit-Checkliste für die RA“)

**„Mystery Shopping“:**
Eine der wichtigsten Tätigkeiten des RO ist die Belehrung des Signators im Sinne des Signaturgesetzes. Diese ist auch ein Qualitätskriterium von a.sign premium. Die diesbezügliche Qualitätskontrolle lässt sich mit „Mystery Shopping“ umsetzen, welches von a.trust durchgeführt wird.

Ergebnisse daraus werden von a.trust ausschließlich an die jeweils verantwortlichen zRO weiter gegeben und mit diesen besprochen.

a.trust überlässt es der RA (aber empfiehlt dies gleichzeitig auch), „Mystery Shopping“ als Maßnahme von intern organisierten Audits umzusetzen.



# Anhang I: Anforderungen an den RO-Arbeitsplatz

**Die technischen Anforderungen an einen RO-Arbeitsplatz sind dem marktüblichen Fortschritt der Computertechnologie unterworfen.**

**Das jeweils den aktuellen Stand der Technik repräsentierende Dokument ist der zRO Download Area von www.a-trust.at („RO Arbeitsplatz“) zu entnehmen.**

# Anhang II: Kennzahlen zur RA-Kosten-Einschätzung

**Die Festlegung der Preise und Konditionen für Registration Authorities obliegt dem Aufsichtsrat der a.trust GmbH.**

**Das jeweils den aktuellen Stand repräsentierende Dokument ist der zRO Download Area von www.a-trust.at („RA Preisliste“)zu entnehmen.**

# Anhang III: Audit-Checkliste für die RA

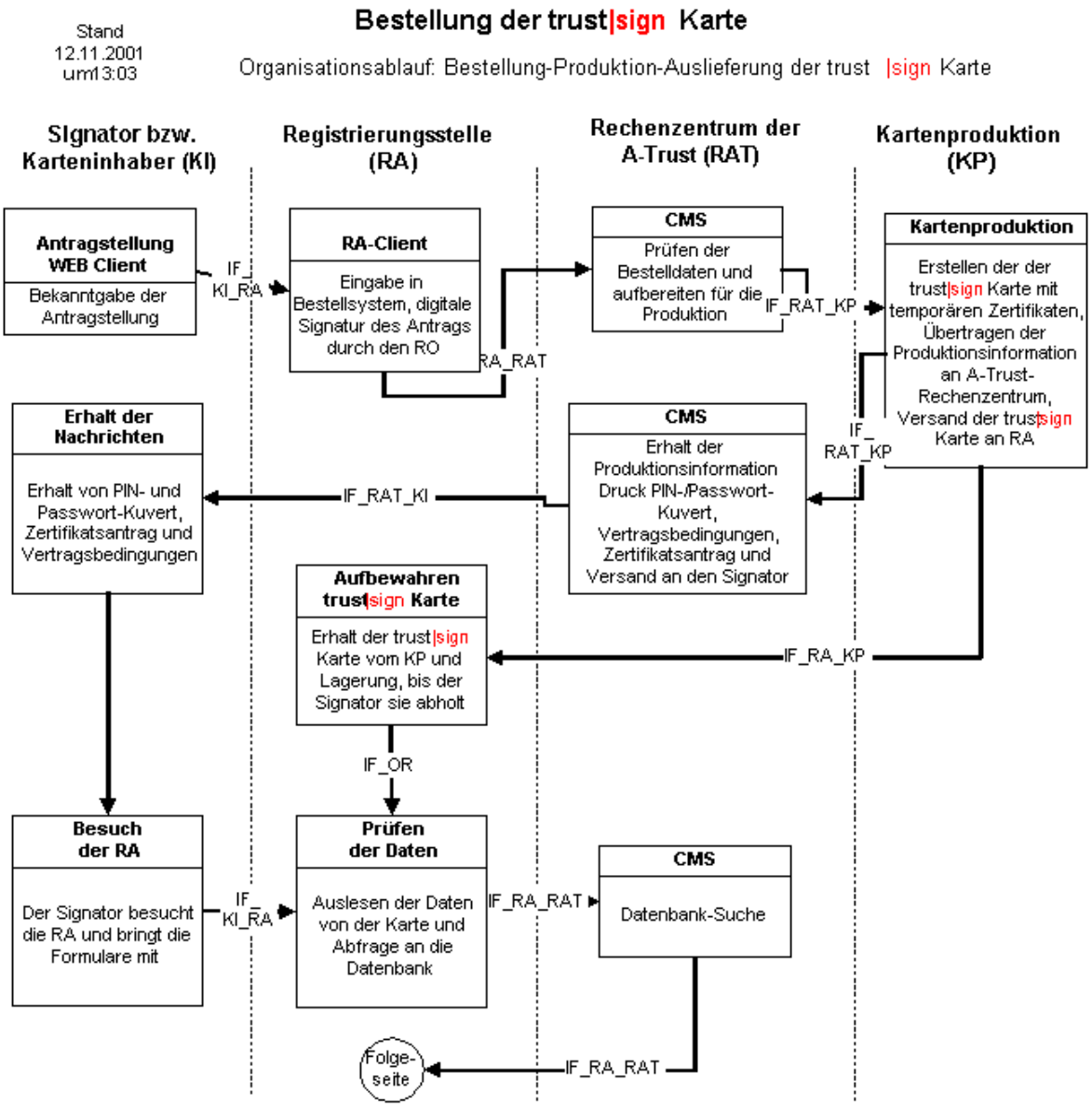
**Die Audit-Checkliste ist die Grundlage für die Überprüfung der Einhaltung des vorliegenden Sicherheitskonzepts in der Praxis.**

**Sie gewährleistet Transparenz und Objektivität der Auditmaßnahmen und dient der einheitlichen Rückmeldung der Auditergebnisse an den zRO und von diesem an a.trust. Aus diesem Grund hält a.trust die Audit-Checkliste als separates Dokument download- und ausdruckbar.**

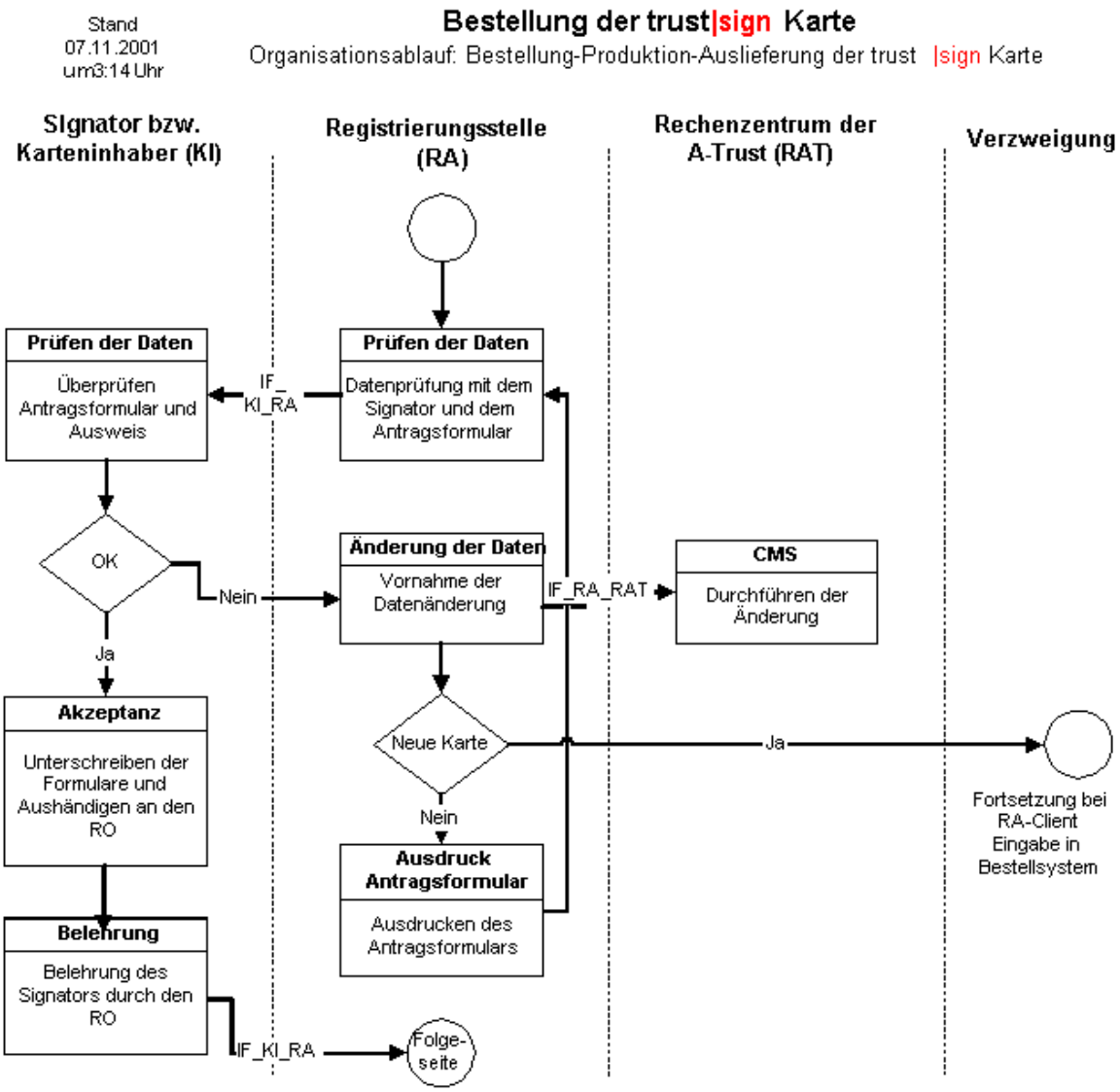
**Das jeweils den aktuellen Stand repräsentierende Dokument ist der RO Download Area von www.a-trust.at „Auditing (Revision)“zu entnehmen.**

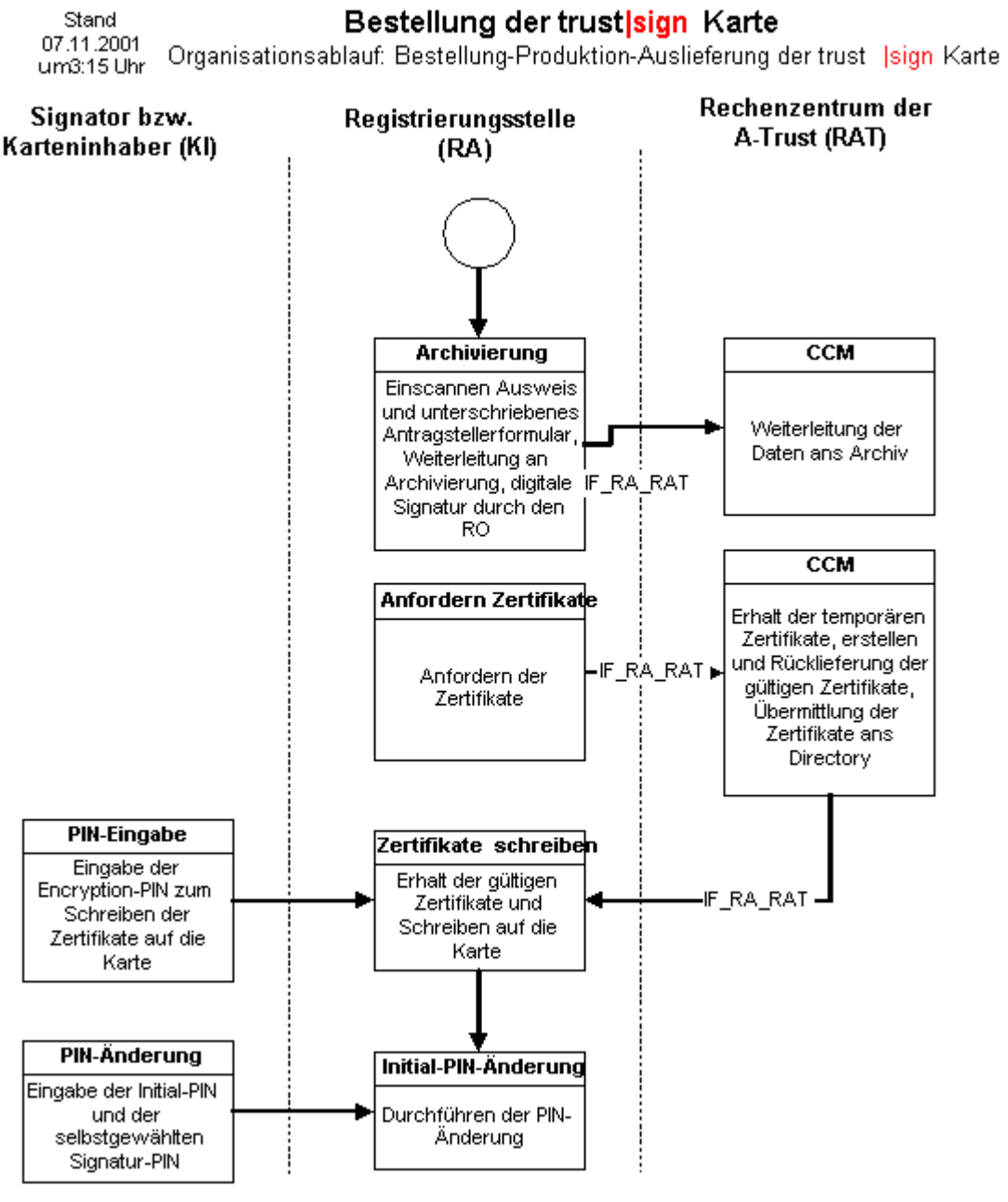
Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

# Anhang IV: Organisationsablauf bei Bestellung der Signaturkarte



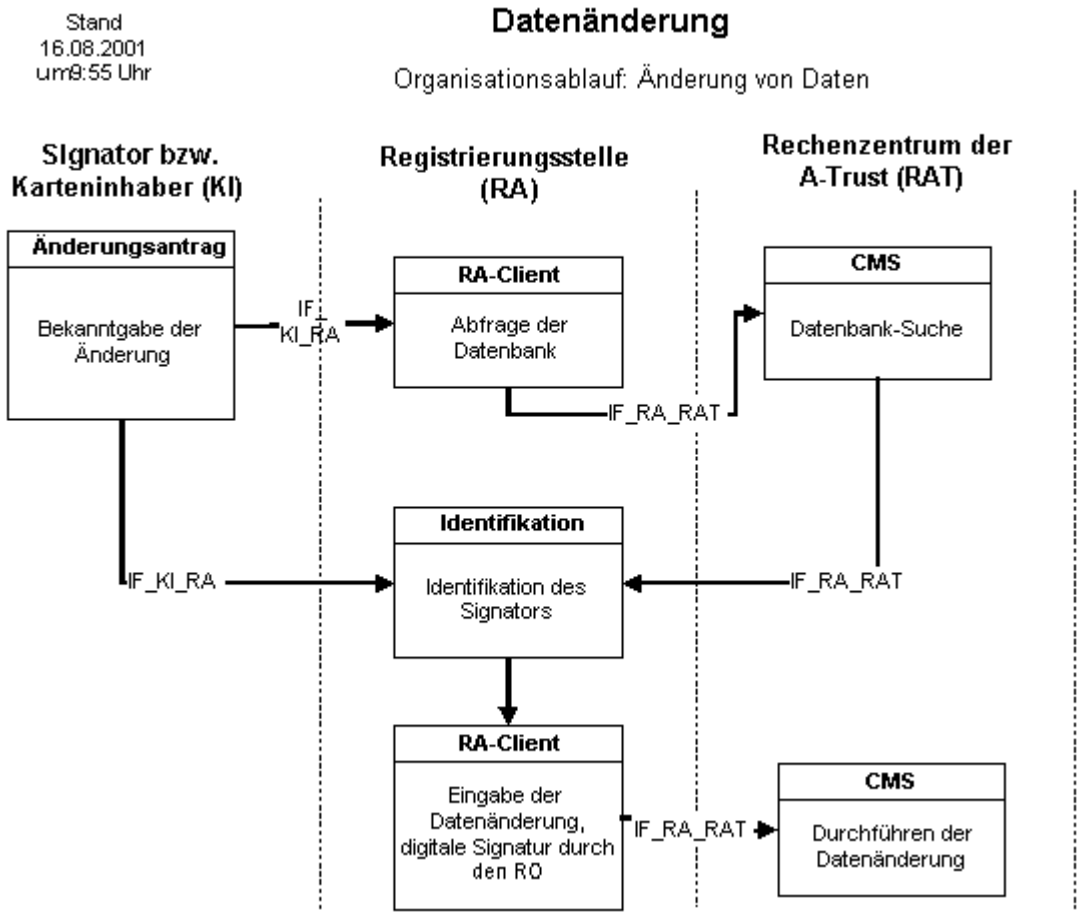

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.


Stand
07.11.2001
um3:14 Uhr
Bestellung der trust|sign Karte
Organisationsablauf: Bestellung-Produktion-Auslieferung der trust |sign Karte
Signator bzw. Karteninhaber (KI)
Registrierungsstelle (RA)
Rechenzentrum der A-Trust (RAT)
Verzweigung
Prüfen der Daten
Überprüfen Antragsformular und Ausweis
IF_KI_RA
Prüfen der Daten
Datenprüfung mit dem Signator und dem Antragsformular
OK
Nein
Ja
Änderung der Daten
Vornahme der Datenänderung
IF_RA_RAT
CMS
Durchführen der Änderung
Akzeptanz
Unterschreiben der Formulare und Aushändigen an den RO
Neue Karte
Ja
Nein
Fortsetzung bei RA-Client Eingabe in Bestellsystem
Ausdruck Antragsformular
Ausdrucken des Antragsformulars
Belehrung
Belehrung des Signators durch den RO
IF_KI_RA
Folge-seite



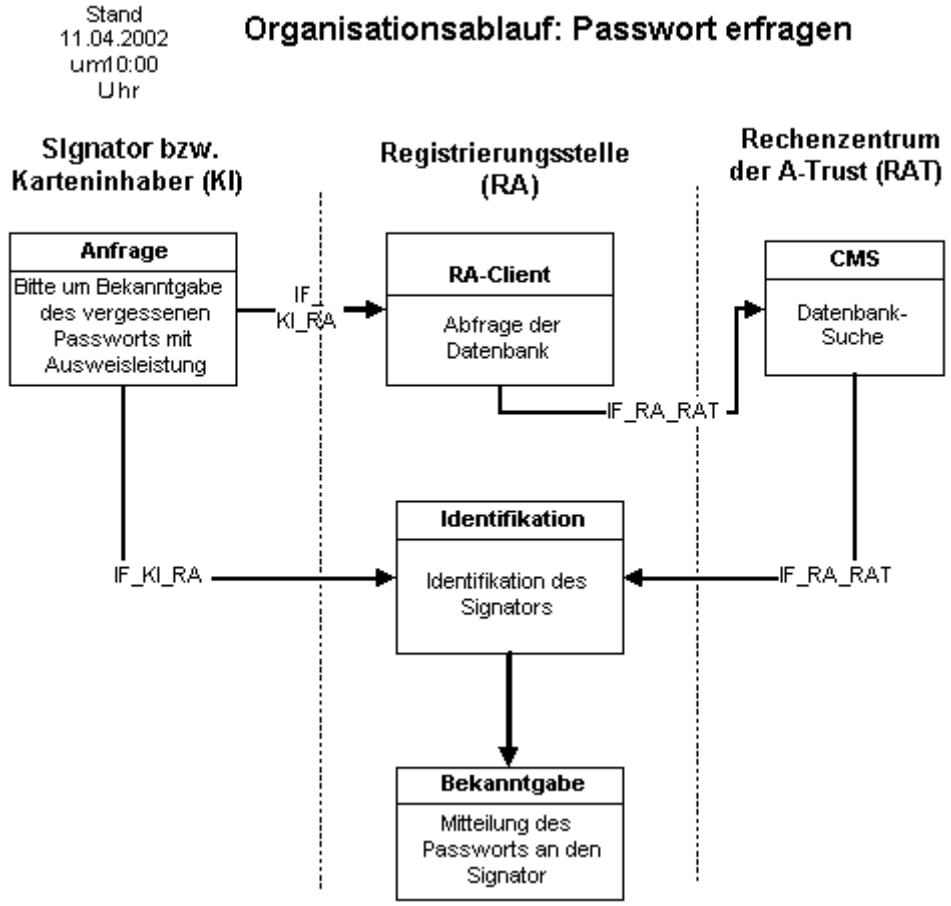

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

# Anhang V: Organisationsablauf bei Datenänderung



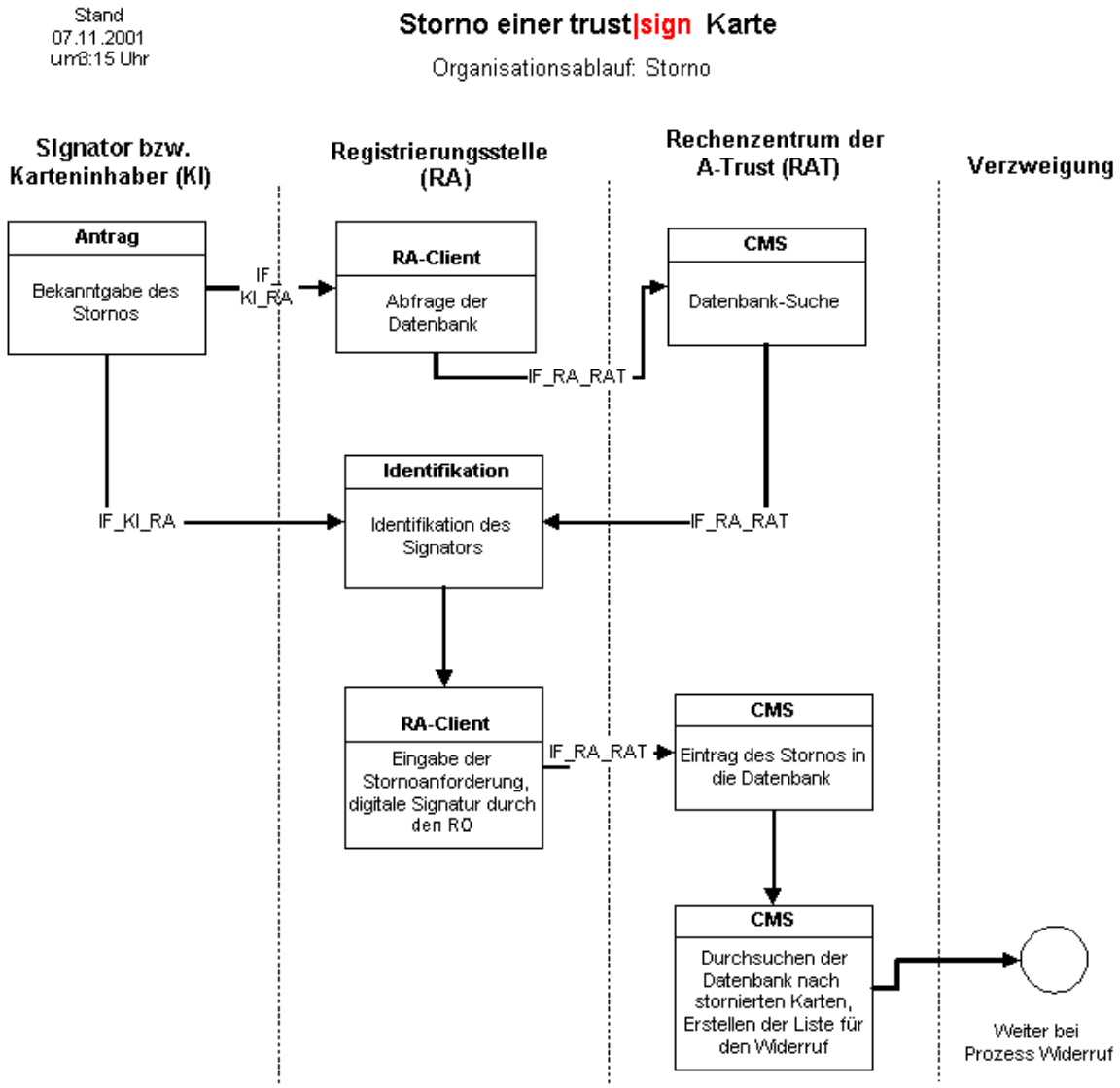

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

# Anhang VI: Organisationsablauf bei Passwort erfragen

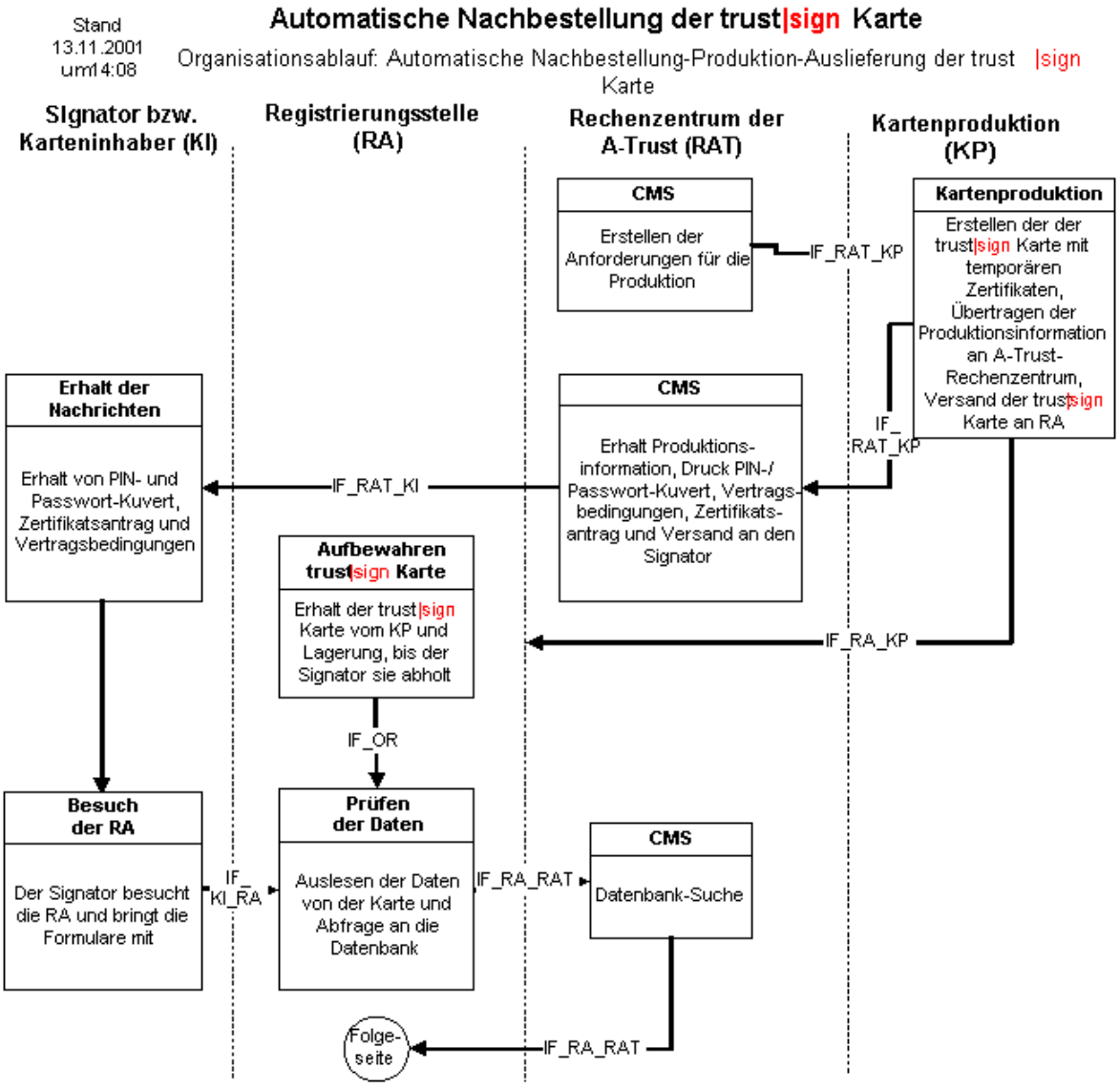



Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.

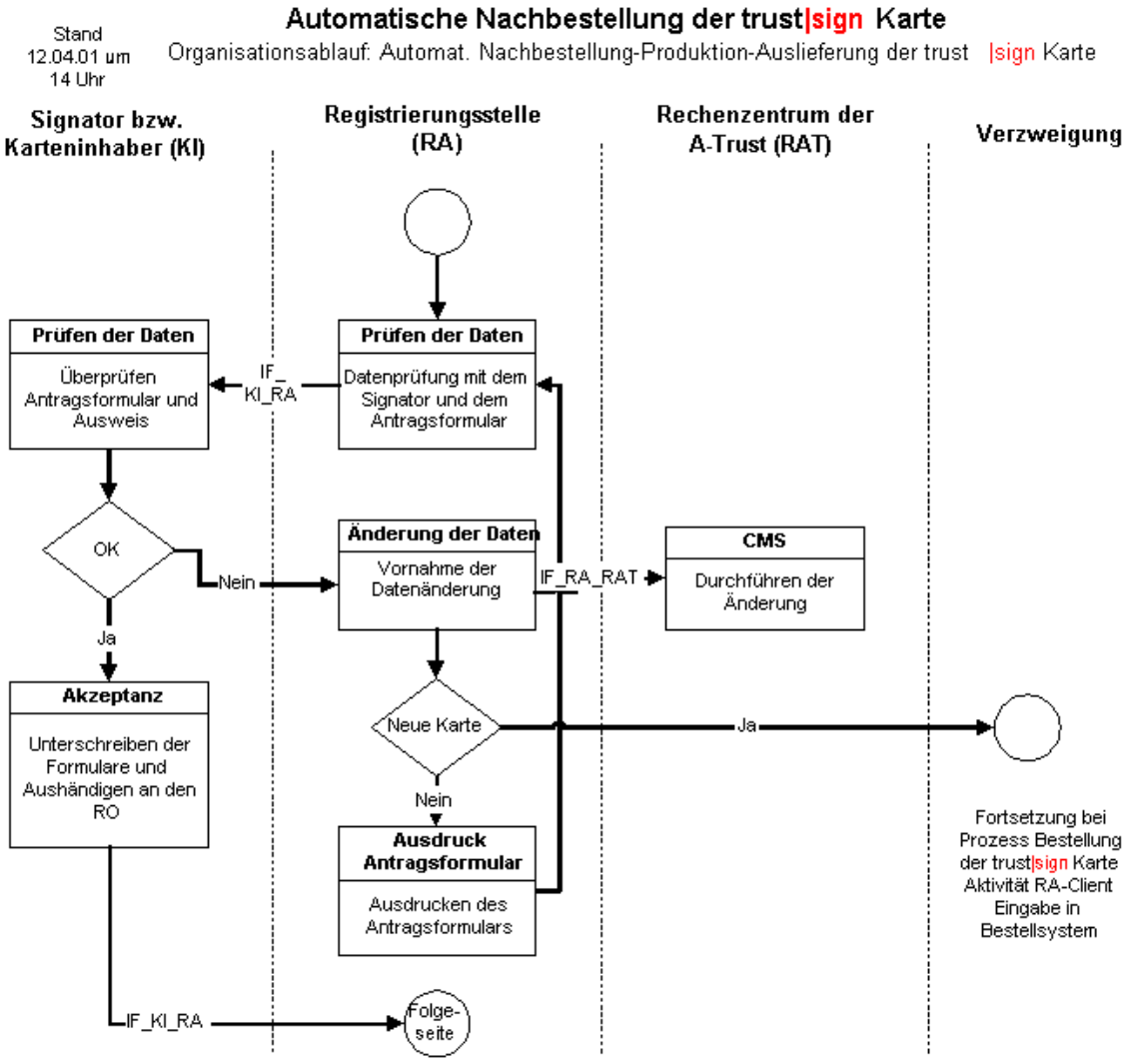
# Anhang VII: Organisationsablauf bei Storno



# Anhang VIII: Organisationsablauf bei automatischer Nachbestellung



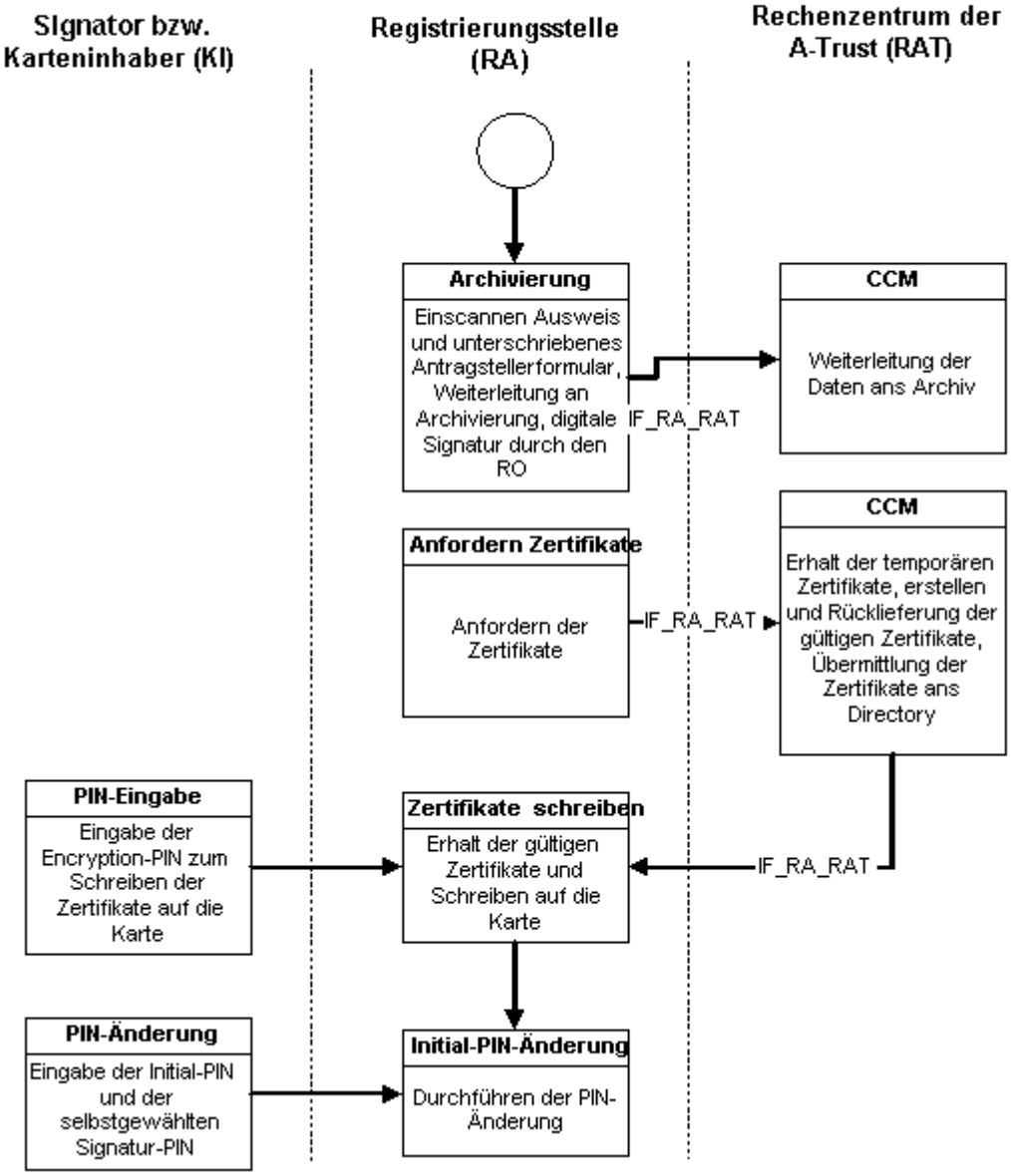

Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.


Automatische Nachbestellung der trust|sign Karte
Stand 12.04.01 um 14 Uhr
Organisationsablauf: Automat. Nachbestellung-Produktion-Auslieferung der trust |sign Karte
Signator bzw. Karteninhaber (KI)
Registrierungsstelle (RA)
Rechenzentrum der A-Trust (RAT)
Verzweigung
Prüfen der Daten
Überprüfen Antragsformular und Ausweis
IF_KI_RA
Prüfen der Daten
Datenprüfung mit dem Signator und dem Antragsformular
OK
Nein
Ja
Änderung der Daten
Vornahme der Datenänderung
IF_RA_RAT
CMS
Durchführen der Änderung
Akzeptanz
Unterschreiben der Formulare und Aushändigen an den RO
Neue Karte
Ja
Nein
Ausdruck Antragsformular
Ausdrucken des Antragsformulars
IF_KI_RA
Folge-seite
Fortsetzung bei Prozess Bestellung der trust|sign Karte Aktivität RA-Client Eingabe in Bestellsystem

Stand
07.11.2001
um3:13 Uhr

## Automatische Nachbestellung der trust|sign Karte

Organisationsablauf: Automat. Nachbestellung-Produktion-Auslieferung der trust|sign Karte




Wir haben in diesem Dokument zur besseren Lesbarkeit auf geschlechtsneutrale Formulierungen verzichtet und bitten dafür um Verständnis.