



## **ELENA-Verfahrensbeschreibung**

**Version 1.0**

1	Einleitung .....	6
1.1	Einführung.....	6
1.2	Das ELENA-Verfahren.....	7
1.2.1	Grundsätzliches .....	7
1.2.2	Vorteile des Verfahrens .....	8
1.2.3	ELENA-Übersicht.....	9
1.3	Designprinzipien der ZSS .....	13
1.3.1	Kommunikation von Innen .....	15
1.3.2	Zonentrennung (horizontal) .....	15
1.3.3	Äußere Sicherheitsschicht .....	16
1.3.4	Innere Sicherheitsschicht.....	16
1.3.5	Vertikale Trennung .....	17
1.3.6	Arbeitgeberseite.....	18
1.3.7	Abrufseite.....	18
1.4	Kommunikation mit externen Stellen .....	18
1.5	Verschlüsselte Speicherung der Daten.....	19
1.5.1	Hardware Security Modul (HSM) .....	19
1.6	Datenschutz und Datensicherheit .....	19
1.6.1	Übergreifend gültige Aspekte .....	20
1.6.1.1	Trennung des Verfahrens in RFV und ZSS (Eckpunktekatalog Punkt 8) ...	20
1.6.1.2	Zuordnung von Versicherungs- bzw. Verfahrensnummer zu VID/ZID nur in der RFV (Eckpunktekatalog Punkt 20).....	20
1.6.1.3	Kein Zugriff von Stellen, die nicht mit den Aufgaben des Anwendungsbereichs § 95 Absatz 1 SGB IV betraut sind (Eckpunktekatalog Punkt 15) .....	20
1.6.1.4	Zweckbindung der Meldedaten (Eckpunktekatalog Punkt 16).....	20
1.6.1.5	Kein Outsourcing der durch das ELENA-Verfahrensgesetz formulierten Aufgaben.....	20
1.6.2	Datenschutz und Datensicherheit bei der RFV.....	21
1.6.2.1	Sicherheitskonzeption des Betriebs nach BSI-Standard .....	21
1.6.2.2	Technische Aufteilung innerhalb der RFV .....	21
1.6.2.3	Dedizierte Hardware-Systeme .....	21
1.6.2.4	Hochverfügbarkeitslösungen .....	21
1.6.2.5	Implementierung von Intrusion Detection/Prevention Methoden .....	21

1.6.2.6	Notfall- und Katastrophenkonzepte.....	21
1.6.2.7	Eigene und unabhängige Entwicklungs-, Test- und Produktionsumgebung .....	22
1.6.2.8	Vier-Augen-Prinzip bei kritischen Prozessen.....	22
1.6.3	Keine Einschränkung bei den verwendeten Signaturkarten (Eckpunktekatalog Punkt 12).....	22
1.6.4	Datenschutz und Datensicherheit bei der ZSS.....	22
1.6.4.1	Sicherheitskonzeption des Betriebs nach BSI-Standard .....	22
1.6.4.2	Umfassende Trennung von ZSS und DSRV (Eckpunktekatalog Punkt 9)..	22
1.6.4.3	Trennung der Verfahren innerhalb der ZSS (Eckpunktekatalog Punkt 3)...	22
1.6.4.4	Dedizierte Hardware-Systeme .....	23
1.6.4.5	Hochverfügbarkeitslösungen .....	23
1.6.4.6	Implementierung von Intrusion Detection/Prevention Methoden .....	23
1.6.4.7	Notfall- und Katastrophenkonzepte.....	23
1.6.4.8	Eigene und unabhängige Entwicklungs-/Test- und Produktionsumgebung	23
1.6.4.9	Vier-Augen-Prinzip bei kritischen Prozessen.....	23
1.6.4.10	Verschlüsselung der Transportwege der Meldedaten (Eckpunktekatalog Punkt 1).....	23
1.6.4.11	Verschlüsselung der Datensätze in der zentralen Datenbank (Eckpunktekatalog Punkt 2).....	24
1.6.4.12	BfDI bei Master-Key Szenario (Eckpunktekatalog Punkt 13).....	24
1.6.4.13	Speicherung der Datensätze nur unter Ordnungsmerkmal vID/ZID (Eckpunktekatalog Punkt 6).....	24
1.6.4.14	Löschen der Datensätze bei Fristablauf (Eckpunktekatalog Punkt 11) ..	24
1.6.4.15	Abruf nur durch zugelassene abrufende Stellen (Eckpunktekatalog Punkt 17).....	24
1.6.4.16	Begrenzung des Datenabrufs (Eckpunktekatalog Punkt 14) .....	25
1.6.4.17	„Zwei-Karten-Prinzip“ zum Abruf der Daten (Eckpunktekatalog Punkt 7).....	25
1.6.4.18	Einverständniserklärung des Teilnehmers mit qualifizierter Signatur (Eckpunktekatalog Punkt 4).....	25
1.6.4.19	Einverständniserklärung durch bevollmächtigte Personen (Eckpunktekatalog Punkt 5).....	25
1.6.4.20	Protokollierung der Datenbanktransaktionen.....	25
	Protokollierung der Arbeitgebermeldungen (Eckpunktekatalog Punkt 18) .....	25

Protokollierung der Datenabrufe (Eckpunktekatalog Punkt 18) .....	26
1.6.4.21    Speicherung der Einverständniserklärungen (Eckpunktekatalog Punkt 19) .....	26
1.6.5    Datenschutz und Datensicherheit bei den abrufenden Stellen .....	26
1.6.5.1    Zweckbindung des Datenabrufs (Eckpunktekatalog Punkt 10) .....	26
2    Verfahrens- und Prozessbeteiligte und deren Aufgaben .....	27
2.1    Aufgaben und Kommunikationsbeziehungen der Verfahrensbeteiligten .....	27
2.1.1    Arbeitgeber und Zentrale Speicherstelle .....	27
2.1.1.1    Meldung des Multifunktionalen Verdienstdatensatzes (MVDS) bei Gehaltsabrechnung.....	27
2.1.1.2    Rückmeldung der Verarbeitungsergebnisse je Sendung.....	30
2.1.1.3    Anforderung einer Versicherungsnummer / Verfahrensnummer .....	31
2.1.1.4    Rückmeldung einer Versicherungsnummer / Verfahrensnummer .....	32
2.1.1.5    Statusabfrage AG (nur lesend) .....	34
2.1.2    Zentrale Speicherstelle und Registratur Fachverfahren .....	34
2.1.2.1    Anforderung vID/ZID .....	34
2.1.2.2    Rückmeldung vID/ZID.....	35
2.1.3    RFV und DSRV.....	36
2.1.3.1    Prüfung der Versicherungs- oder Verfahrensnummer nach Meldung des MVDS .....	36
2.1.3.2    Rückmeldung nach Prüfung der Versicherungsnummer .....	36
2.1.3.3    Anmeldung eines Teilnehmers .....	37
2.1.4    Teilnehmer und ZSS.....	37
2.1.4.1    Widerruf Einverständnis.....	37
2.1.5    Abrufende Stelle und ZSS .....	37
2.1.6    ZSS und DSRV .....	37
2.1.6.1    Anforderung einer Versicherungsnummer / Verfahrensnummer .....	37
2.1.6.2    Rückmeldung der Versicherungsnummer / Verfahrensnummer.....	38
2.1.7    ZSS und AG-Trustcenter .....	42
2.1.7.1    Verifizieren Arbeitgeberschlüssel.....	42
2.1.8    ZSS und Trustcenter.....	42
2.1.8.1    Verifizieren der Zertifikatsdaten bei Abruf.....	42
2.1.9    Abrufende Stelle und Trustcenter .....	42
3    Verarbeitungsprozesse .....	43
3.1    Verarbeitung eines MVDS .....	43

3.1.1	Meldung des MVDS bei Gehaltsabrechnung.....	43
3.2	Verarbeitung eines DSVV .....	45
3.2.1	Bekanntgabe einer vergebenen Verfahrensnummer an den Teilnehmer.....	48
3.3	ZSS zu abrufenden Stellen .....	49
3.4	ZSS mit RFV und DSRV .....	49
3.4.1	Prüfung der Versicherungs- bzw. Verfahrensnummer nach Meldung des MVDS.....	49
3.4.1.1	DSRV Kommunikationszustände.....	51
3.4.1.2	Kommunikationsprotokoll.....	53
3.4.2	Anfrage zur Vergabe einer VID/ZID zu einer Versicherungsnummer/Verfahrensnummer.....	54
3.4.2.1	Vergabe einer VID .....	55
3.4.3	Bekanntgabe einer vergebenen Verfahrensnummer an den Teilnehmer.....	56
4	Löschung der Daten ( <i>Dieses Kapitel ist noch zu erstellen</i> ).....	57
4.1	ZSS.....	57
4.2	RFV.....	57
5	Anlagen .....	57
6	Anhänge.....	58
6.1	Begriffsdefinitionen .....	58
6.2	Tabellenverzeichnis .....	58
6.3	Abbildungsverzeichnis .....	58

# 1 Einleitung

## 1.1 Einführung

Der Bundestag hat am 28.03.2009 mit Zustimmung des Bundesrates das Gesetz über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) beschlossen (**vgl. Anlage 1**). Das Gesetz wurde am 01.04.2009 im Bundesgesetzblatt (Teil I Nr. 17, Seite 634) veröffentlicht und ist am Tag darauf in Kraft getreten. Das BMAS wird gemäß § 97 Absatz 6 SGB IV die ELENA-Datensatzverordnung erlassen (**vgl. Anlage 2**). Der Verordnungsentwurf ist vom BMAS fertig. Eine Zuleitung kann aber erst zur 1. Sitzung des Bundesrates am 12. Februar 2010 erfolgen, da die Ressortabstimmung sich verzögert hat. Das Verfahren wird dadurch nicht behindert, da sowohl die gesetzliche Verpflichtung zur Meldung ab 1. Januar 2010 besteht, wie auch die technischen Grundsätze für die Meldungen verbindlich beschlossen sind.

Weitere Grundlagen sind die

- Gemeinsamen Grundsätze für die Erstattung der Meldungen der Arbeitgeber an die Zentrale Speicherstelle im Rahmen des Verfahrens des elektronischen Entgeltnachweises nach § 28b Absatz 6 SGB IV (**vgl. Anlage 3a**)
- Gemeinsamen Grundsätze zur Kommunikation zwischen der Zentralen Speicherstelle, der Registratur Fachverfahren und der Datenstelle der Träger der Rentenversicherung nach § 28b Absatz 6 SGB IV (**vgl. Anlage 3b**)
- Gemeinsame Grundsätze zur Kommunikation zwischen den ZSS und den abrufenden Stellen (**vgl. Anlage 3c**)

Die vorliegende Verfahrensbeschreibung wurde gemeinsam von der Zentralen Speicherstelle (ZSS), der Registratur Fachverfahren (RFV) und den abrufenden Stellen

entwickelt. Ziel dieses Dokumentes ist eine umfassende Beschreibung des ELENA-Verfahrens. Es dient als Basis für die nicht öffentlichen Feinkonzepte der Beteiligten. Es setzt die Kenntnis der allgemeinen Verfahrensweise voraus. In der im Anhang 6.1 beigefügten Tabelle werden Begriffe erklärt, die im vorliegenden Dokument häufiger verwendet werden.

Die Verfahrensbeschreibung ist so konzipiert, dass sie die einzelnen Einsatztermine des Verfahrens berücksichtigt. Die vorliegende Version 1.0 berücksichtigt die Datenannahme ab 01.01.2010. Belange der abrufenden Stellen werden in der Version 2.0 ab 01.07.2010 berücksichtigt.


## **1.2 Das ELENA-Verfahren**

### **1.2.1 Grundsätzliches**

Mit dem ELENA-Verfahren will der Gesetzgeber eine erhebliche Entlastung der Wirtschaft von Bürokratiekosten erreichen und innovativ für eine breite Anwendung von qualifizierten Signaturen sorgen, die die Rechtssicherheit im Bereich der elektronischen Kommunikation sicherstellen. Es wird den Arbeitgebern ermöglichen, künftig auf das Ausstellen von schriftlichen Entgeltbescheinigungen zu verzichten und stattdessen monatlich Entgeltdaten an eine Zentrale Speicherstelle zu melden.

Von der Zentralen Speicherstelle (ZSS), die bei der Datenstelle der Träger der Rentenversicherung (DSRV) in Würzburg eingerichtet ist, werden die jeweils berechtigten abrufenden Stellen bei Bedarf und unter Mitwirkung des Teilnehmers die erforderlichen Daten abrufen können, um auf deren Grundlage entsprechende Leistungen zu berechnen.

Aus Datenschutzgründen ist allerdings eine strikte Trennung der Aufgaben und Daten der ZSS von den übrigen Aufgaben und Datenbeständen der Rentenversicherung zu gewährleisten, was dadurch bewerkstelligt wird, dass die ZSS räumlich, personell und insbesondere organisatorisch von den übrigen Datenbeständen der Deutschen Rentenversicherung Bund getrennt aufgebaut wird (vgl. § 96 Absatz 1 SGB IV). Außerdem wird eine „Registratur Fachverfahren“ bei der Informationstechnischen Servicegesellschaft der gesetzlichen Krankenversicherung (ITSG) eingerichtet (vgl. § 96 Absatz 2 SGB IV).

	<b>ELENA</b> <b>Verfahrensbeschreibung</b>	Seite: 8 Stand: <b>01.01.2010</b> Version: <b>1.0</b>
---	---	---

Diese Stelle ermöglicht die Zuordnung der Zertifikatsdaten der Signaturkarten zu den entsprechenden Daten des Teilnehmers.

Der Aufbau der Infrastruktur ist abgeschlossen, so dass die Arbeitgeber ab 01.01.2010 Meldungen für Arbeitnehmer übermitteln. Datenabrufe im Rahmen von ELENA werden ab 2012 mit Bescheinigungen aus dem Bereich Arbeitslosengeld, Bundeseltern geld und Wohngeld eingeführt.

### 1.2.2 Vorteile des Verfahrens

Das ELENA-Verfahren bringt Nutzen für:

- Bürokratieabbau
- Vermeidung von Leistungsmissbrauch
- Entlastung des Arbeitgebers
- Teilnehmer

Das ELENA-Verfahren fördert darüber hinaus die Verbreitung der qualifizierten Signaturen. Mit ELENA ist ein wichtiger Grundstein für den weiteren Bürokratieabbau gelegt. Es bietet zum einen für die Sozialleistungsbehörden die Chance, ihre Verfahren zu optimieren und weitgehend automatisiert zu gestalten und zum anderen einen optimalen Service für den Bürger für gerechte, fehlerfreie und rasche Leistungsfestsetzung. ELENA wird in Ausbaustufen - wenn alle Sozialleistungen einbezogen sind - geeignet sein, den Leistungsmissbrauch weitgehend auszuschließen.

Nach Schätzungen des Normenkontrollrates wird ELENA den Arbeitgebern ab 2012 Einsparungen von jährlich ca. 86 Mio. Euro bringen.

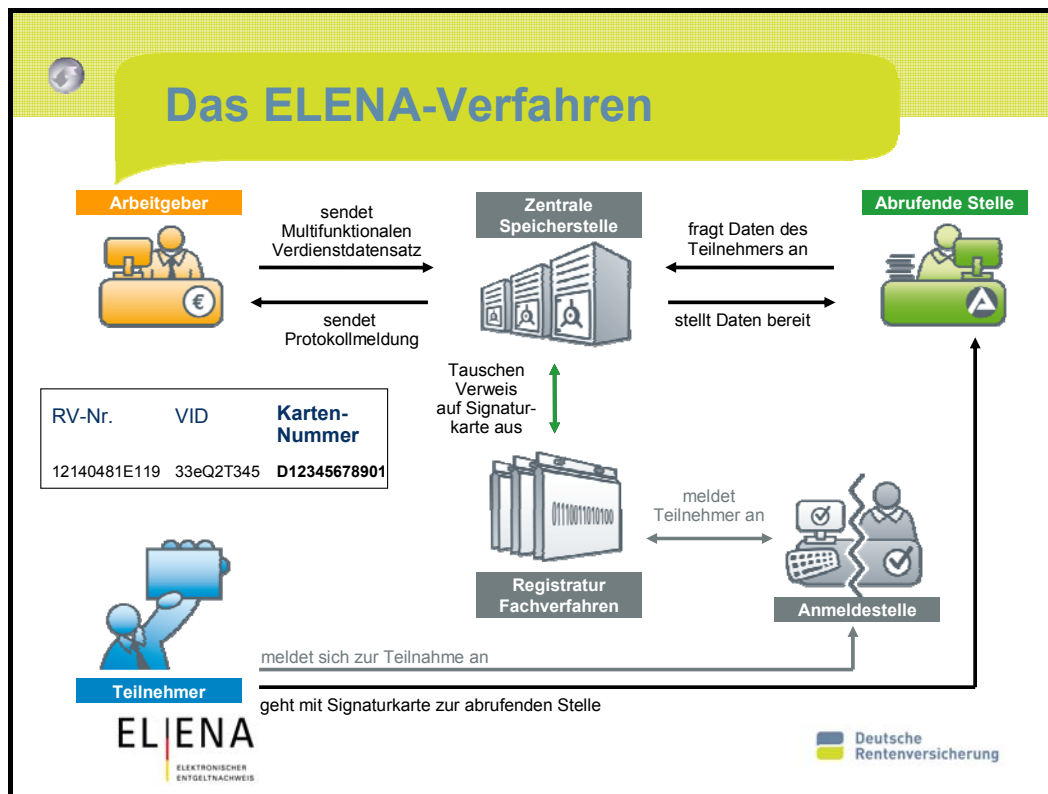
Auch der Teilnehmer hat Vorteile aus dem Verfahren, da er künftig die Gewissheit haben wird, dass der Arbeitgeber den Grund für die notwendige Ausstellung einer Bescheinigung nicht kennt. Er muss also seine persönlichen Verhältnisse nicht offen legen. Weiterhin werden die Prozesse in der öffentlichen Verwaltung beschleunigt, Fehler vermieden und derzeit vorhandene Medienbrüche beseitigt. Das macht den öffentlichen Sektor zu einem bürgernahen Dienstleister, der die Beratung intensivieren kann.



Durch die multifunktionalen Verwendungsmöglichkeiten einer Signaturkarte (Smartcard) können sukzessive weitere Anwendungen - auch außerhalb des gesetzlichen Melde- und Bescheinigungswesens - entwickelt und realisiert werden. Dieser Mehrfachnutzen steigert die Akzeptanz des ELENA-Verfahrens bei allen Beteiligten und in der Öffentlichkeit. Für Unternehmen entsteht ein neuer Markt. Eine einheitliche Schnittstelle zur Signaturkarte (eCard-API) sorgt für Investitionssicherheit und fördert einen attraktiven Wettbewerb.

### 1.2.3 ELENA-Übersicht

Im ELENA-Verfahrensgesetz werden fünf Entgeltbescheinigungen mit den zugehörigen Verwaltungsprozessen behandelt (§ 95 Absatz 1 SGB IV). Die Entgeltbescheinigungsdaten werden von den Arbeitgebern in Form eines multifunktionalen Verdienstdatensatzes (MVDS) gemeldet. Dieser Datensatz wird in der ZSS syntaktisch und semantisch geprüft und verschlüsselt abgelegt. Die abrufenden Stellen holen sich mit Einverständnis des Teilnehmers die für sie relevanten Entgeltdaten ab, die von der Zentralen Speicherstelle bereitgestellt werden. In der nachfolgenden **Abbildung 1** werden im Überblick die beteiligten Personen und Systeme skizziert.



**Abbildung 1: Gesamtüberblick ELENA-Verfahren**

Der Arbeitgeber meldet künftig monatlich gleichzeitig mit der Entgeltabrechnung die Arbeitnehmerdaten an die ZSS. Der ordnungsgemäße Eingang der Daten wird elektronisch quittiert. Aus dieser zentralen Speicherstelle können die jeweils berechtigten abrufenden Stellen bei Bedarf und unter Mitwirkung des Teilnehmers die erforderlichen Daten abrufen, um auf deren Grundlage entsprechende Leistungen zu berechnen.

Dies setzt voraus, dass sich der Teilnehmer eine Chipkarte mit einer qualifizierten Signatur beschafft, da es ohne diesen digitalen Schlüssel künftig keinen Zugang zu den staatlichen Leistungen geben wird, die in das ELENA-Verfahren eingebunden sind.

Die einzelnen Aufgaben der Beteiligten sind in der nachfolgenden **Tabelle 1** näher definiert bzw. beschrieben.

Arbeitgeber	Der Arbeitgeber erstellt nach § 97 SGB IV monatlich für jeden seiner abhängig Beschäftigten einen multifunktionalen Verdienstdatensatz (MVDS) oder beauftragt jemanden, wie z. B. externe Dienstleister, mit dessen regelmäßiger Erstellung. Er sendet den Datensatz verschlüsselt und authentisiert an die ZSS. Daraufhin erhält er eine Protokollmeldung über die Verarbeitung des Datensatzes. Hierzu wird ein sog. „Abrufserver“ in der ZSS installiert, von der der Arbeitgeber die Statusmeldung seiner Meldungen abholen kann. Die Übermittlung der Daten erfolgt nach den Techniken des DEÜV-Verfahrens.
Zentrale Speicherstelle (ZSS)	Die ZSS (§ 99 SGB IV) speichert die Bestandteile des MVDS verschlüsselt und übermittelt die daraus ermittelbaren Entgeltbescheinigungen, bei Vorliegen einer Einverständniserklärung des Teilnehmers, an die abrufenden Stellen. Die ZSS betreibt unter anderem den Berechtigungsserver. Auf dem Berechtigungsserver werden die Berechtigungen für die Verantwortlichen, Verfahrensverantwortlichen und Sachbearbeiter oder Abrufagent der abrufenden Stellen vorgehalten.
Abrufende Stellen	Die abrufende Stelle (§ 102 SGB IV) ruft die erforderlichen

	<p>Entgeltbescheinigungsdaten von der ZSS ab und verarbeitet diese weiter. Die Einverständniserklärung des Teilnehmers zum Datenabruf ist zwingend erforderlich.</p> <p>Sachbearbeiter bzw. Abrufagent:      Der Sachbearbeiter bearbeitet den Antrag des Teilnehmers und benötigt dazu unter anderem eine oder mehrere Entgeltbescheinigungen. Diese kann er nach erteilter Einverständniserklärung durch den Teilnehmer und wenn er von seinem Verantwortlichen oder Verfahrensverantwortlichen dazu ermächtigt wurde, von der ZSS abrufen. Der Sachbearbeiter bzw. Abrufagent benötigt keine qualifizierte elektronische Signatur!</p> <p>Verantwortlicher:      Jede abrufende Stelle hat einen Verantwortlichen (Root), dessen Aufgabe es ist, die Berechtigungen der seiner Stelle zugeordneten Sachbearbeiter, Abrufagenten und Verfahrensverantwortlichen zu verwalten. Der Verantwortliche teilt der ZSS mit, welcher Sachbearbeiter bzw. Abrufagent Zugriff auf Bescheinigungen erhalten dürfen, welche Bescheinigungen sie abrufen und für welchen Zeitraum sie für diese Abrufe legitimiert sind. Darüber hinaus kann er Berechtigte sperren und somit die Abrufberechtigung entziehen.</p>
<p>Trustcenter        (Zertifizierungsdiensteanbieter)</p>	<p>Die <b>Zertifizierungsdiensteanbieter</b> (§ 7 Absatz 1 Nr. Signaturgesetz) erstellen Schlüssel und Zertifikate für die am System beteiligten Parteien, insbesondere für die Teilnehmer und die Verantwortlichen der abrufenden Stellen. Die <b>Zertifizierungsdiensteanbieter</b> geben die Smartcards aus, mit denen qualifiziert elektronisch signiert werden kann und betreiben die zugehörigen Verzeichnisdienste. Die Verzeichnisdienste erlauben jederzeit eine Überprüfung der Gültigkeit von Zertifikaten mittels Sperrlisten- oder OCSP-Abfragen. Jeder <b>Zertifizierungsdiensteanbieter</b> hat seine</p>

	<p>Registrierungsstellen, die den Empfänger einer Signaturkarte in einem definierten Verfahren (gemäß den Vorgaben der BNetzA (Bundesnetzagentur)), der Zulassung als akkreditiertes oder angezeigtes Trustcenter und den eigenen Trustcenter-spezifischen Sicherheitsrichtlinien) identifizieren.</p>
Teilnehmer	<p>Beschäftigte, Beamte, Richter und Soldaten haben sich nach § 98 Absatz 1 SGB IV zum Verfahren anzumelden, sobald ein erfasster Nachweis erforderlich wird. Mit dieser Anmeldung oder mit der ersten Meldung durch den Arbeitgeber nach § 97 Absatz 1 SGB IV werden diese Teilnehmer am Verfahren.</p> <p>Der Teilnehmer kann sich im Verfahren vertreten lassen. Handelt ein Vertreter für den Teilnehmer, muss er sich zum Verfahren anmelden.</p>
Registratur Fachverfahren (RFV)	<p>Die RFV stellt nach § 100 SGB IV die Verbindung zwischen der Versicherungsnummer und der Zertifikatsidentitätsnummer (ZID) des Teilnehmers her oder vergibt ersatzweise eine vorläufige Identitätsnummer (vID) und stellt diese der ZSS zur Verfügung.</p>

Tabelle 1: Die Aufgaben der Beteiligten

### 1.3 Designprinzipien der ZSS

Die ZSS ist in vier Sicherheitszonen unterteilt, deren einzelnen Funktionen im Folgenden kurz dargestellt werden. Die nachfolgende Abbildung zeigt dies im Überblick.

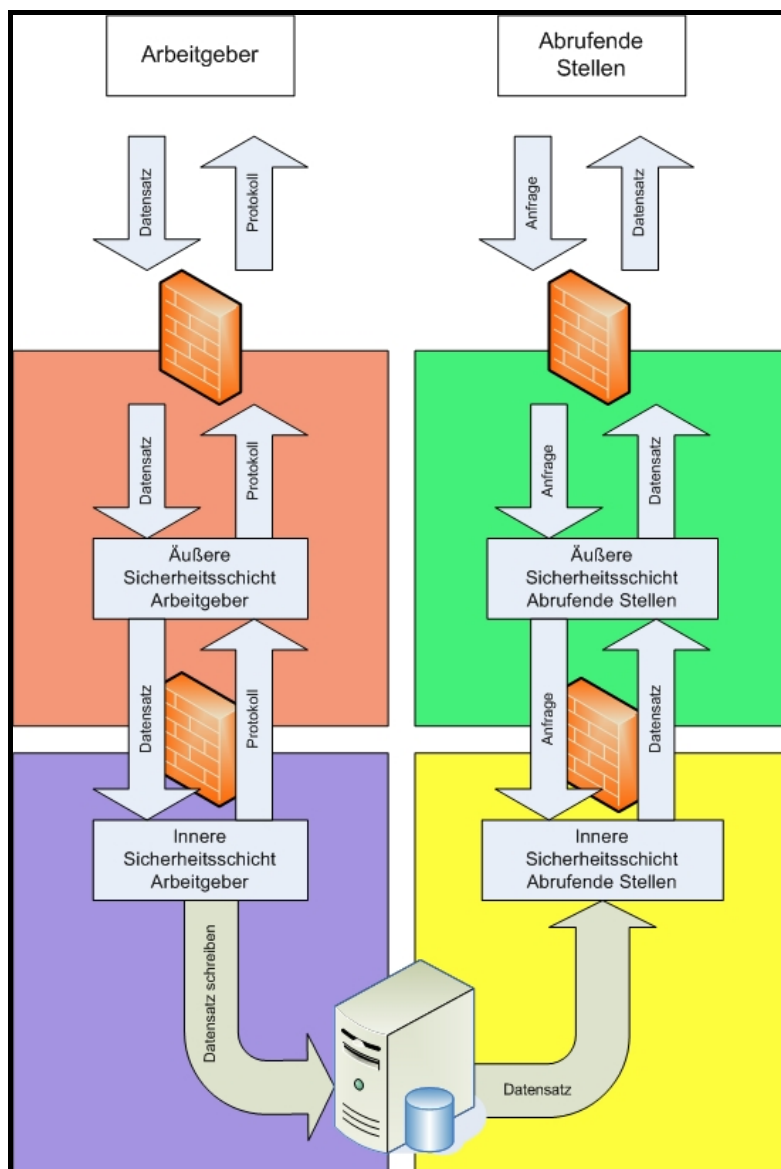


Abbildung 2: Sicherheitszonen ZSS

- Äußere Sicherheitsschicht Arbeitgeber (ÄSS-AG)**  
 Die Äußere Sicherheitsschicht der Arbeitgeber stellt die Annahmesysteme für die Arbeitgebermeldungen bereit. Die Meldedaten liegen hier ausschließlich in verschlüsselter Form vor. Die Schnittstellen in das Internet (externe Schnittstelle) sowie in die Innere

Sicherheitsschicht Arbeitgeber (interne Schnittstelle) sind mittels Firewalls geschützt.

- **Innere Sicherheitsschicht Arbeitgeber (ISS-AG)**

In der Inneren Sicherheitsschicht Arbeitgeber werden die Daten entschlüsselt, überprüft und anschließend wieder verschlüsselt. Danach erfolgt eine Ablage der Daten in der zentralen Datenbank.

- **Äußere Sicherheitsschicht Abrufende Stellen (ÄSS-AS)**

Die Äußere Sicherheitsschicht Abrufende Stellen stellt die Abrufsysteme für die Meldedaten bereit, über die die abrufenden Stellen (z.B. Arbeitsagenturen) Zugriff auf die gespeicherten Daten erhalten. Die Schnittstellen in das Internet (externe Schnittstelle) sowie in die innere Sicherheitsschicht der Abrufseite (interne Schnittstelle) sind mittels Firewalls geschützt.

- **Innere Sicherheitsschicht Abrufende Stellen (ISS-AS)**

In der Inneren Sicherheitsschicht Abrufende Stellen werden die Anfragen der abrufenden Stellen überprüft und, sofern die Anfragen gültig sind, die Daten aus der zentralen Datenbank gelesen und gesichert an die anrufenden Stellen übermittelt.

### 1.3.1 Kommunikation von Innen

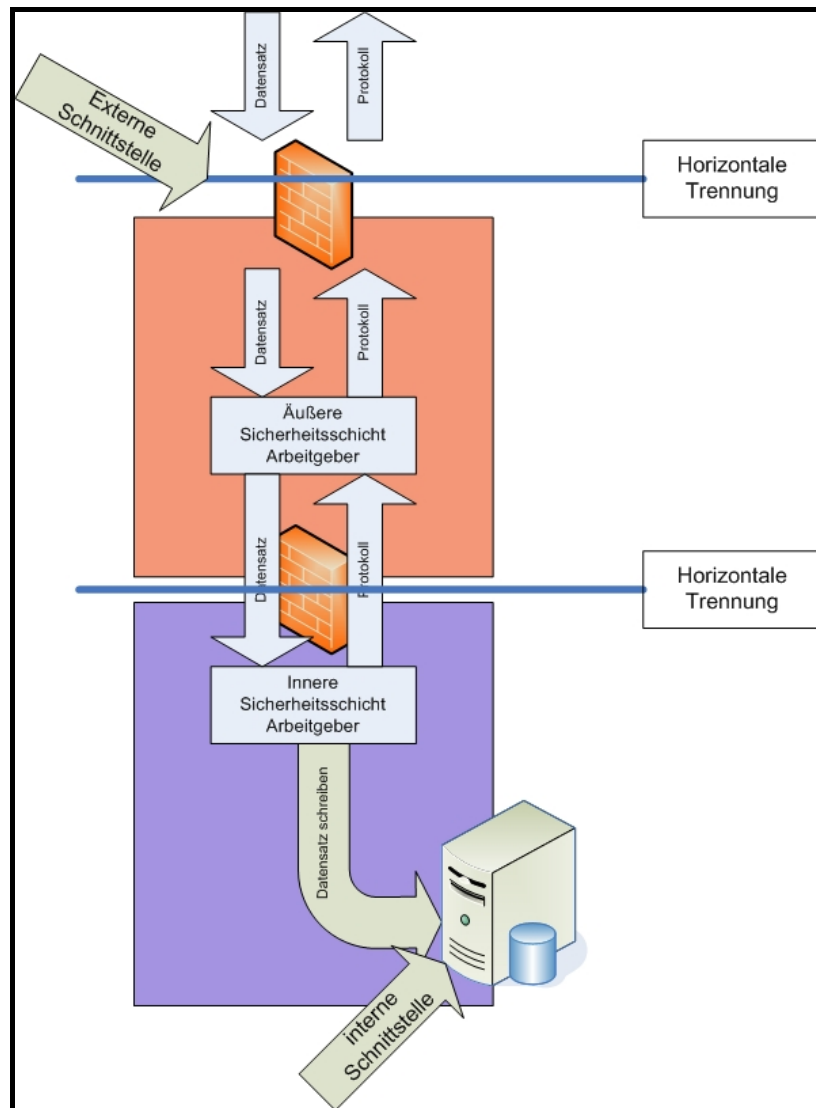
Es existiert keine direkte Kommunikationsmöglichkeit von den Systemen der äußeren in die innere Sicherheitsschicht. Daten, die von der äußeren Sicherheitsschicht in die innere Sicherheitsschicht transferiert werden müssen, müssen aktiv von den Systemen der inneren Sicherheitsschicht abgeholt werden. Es findet somit immer eine Kommunikation von einem sichereren Netzwerkbereich in einen unsichereren Netzbereich statt, nie umgekehrt.

Direkte Kommunikation auf die Systeme der einzelnen Netzbereiche findet aus dem Administrations-Netzwerk heraus statt. Hierbei ist durch technische Maßnahmen sichergestellt, dass keine zonenübergreifende Kommunikation stattfindet.

### 1.3.2 Zonentrennung (horizontal)

Die Arbeitgeber-Seite der ZSS besitzt eine interne Schnittstelle an die zentrale Datenbank sowie eine externe Schnittstelle in das Internet. Im Datenbanksystem sind die geheim zu haltenden Datensätze gespeichert, über das Internet müssen bestimmte Informationen abgerufen bzw. die Datensätze eingeliefert und Rückmeldungen abgerufen werden.

Um eine saubere und sichere Trennung zwischen dem Internet und der zentralen Datenbank zu erreichen, wird bei der ZSS zwischen einer äußeren Sicherheitsschicht und einer inneren Sicherheitsschicht unterschieden. Die Trennung erfolgt zum einen über technische Systeme (Firewalls), zum anderen mittels des Zugriffs-Prinzips (Reverse Proxy).



**Abbildung 3: Horizontale Trennung**

### 1.3.3 Äußere Sicherheitsschicht

Die äußere Sicherheitsschicht ist wie folgt charakterisiert:

- Kommunikation mit externen Systemen wie
  - Verzeichnisdienst
  - Arbeitgebern
  - Abrufende Stellen
- Vom Internet aus erreichbar
- Keine Möglichkeit zur aktiven Kommunikation in die innere Sicherheitsschicht

### 1.3.4 Innere Sicherheitsschicht

Die innere Sicherheitsschicht zeichnet sich durch folgende Merkmale aus:

- Kommunikation mit dem Datenbanksystem

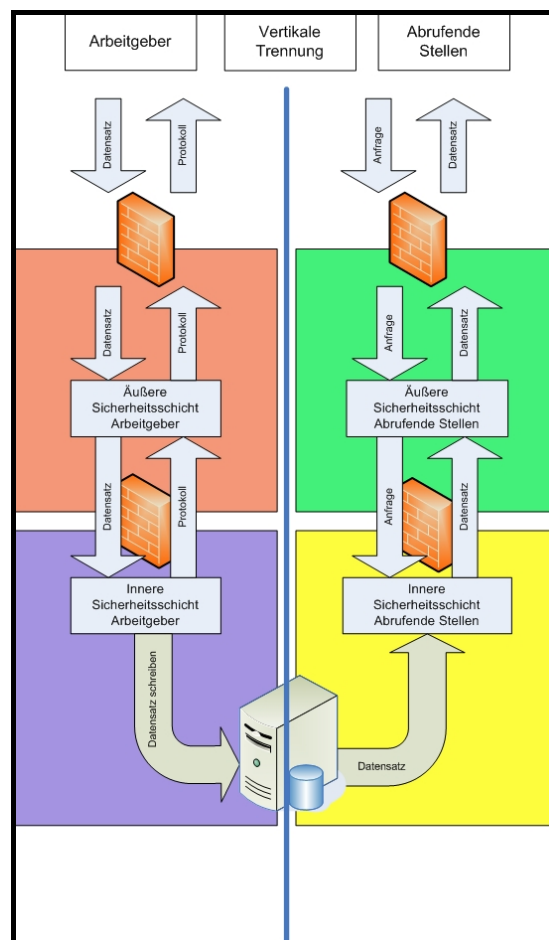


- Kommunikation mit der Registratur Fachverfahren und der DSRV (Direkte Kommunikation über definierte Schnittstellen)
- Einzige Stelle, an der Daten (kurzzeitig) unverschlüsselt vorliegen
- Kein direkter externer Zugriff (z.B. ins Internet) möglich
- Definierter Zugriff auf die Rechner der äußeren Sicherheitsschicht möglich

### 1.3.5 Vertikale Trennung

In das Datenbanksystem werden Daten eingestellt und Daten werden abgerufen. Beide Vorgänge sind getrennt zu halten. So kann schon rein auf Netzwerkebene ein lesender Zugriff auf die Datenbank nur von der berechtigten Seite aus erfolgen, wenn entsprechende Systeme zum Einsatz kommen.

Arbeitgeber senden die Entgeltdaten elektronisch, diese werden von der sogenannten „Arbeitgeberseite“ aus in die zentrale Datenbank geschrieben. Abrufende Stellen rufen Bescheinigungen ab, stellen aber keine Daten ein. Dies ist die sogenannte „Abrufende Stellen Seite“ oder „Abrufseite“, wie in nachfolgender Abbildung 4 veranschaulicht wird.



**Abbildung 4: Vertikale Trennung**

### **1.3.6 Arbeitgeberseite**

Die Arbeitgeberseite ist folgendermaßen charakterisiert:

- Die Daten werden gemäß den gemeinsamen Grundsätzen an die ZSS geliefert.
- Auf der Arbeitgeberseite können die Datensätze nur in die zentrale Datenbank geschrieben werden. Ein Lesen der Daten ist nicht möglich.

### **1.3.7 Abrufseite**

Die Abrufseite zeichnet sich durch folgende Merkmale aus:

- Die Daten werden den abrufberechtigten Stellen in einem Online-Verfahren zur Verfügung gestellt.
- Von der Abrufseite aus können Daten in die zentrale Datenbank nur gelesen, keinesfalls geschrieben werden.

## **1.4 Kommunikation mit externen Stellen**

Die ZSS kommuniziert mit externen Stellen beispielsweise mit

- der Registratur-Fachverfahren (RFV) zum Abruf der Zertifikatsidentifikationsnummer,
- der ITSG zur Abfrage der Arbeitgeber-Zertifikate,
- der DSRV zur Vergabe einer Verfahrensnummer.

Soweit es sich bei den übertragenen Daten um Informationen handelt, die keine besonderen Anforderungen an die Integrität und Vertraulichkeit stellen, wird die Kommunikation über die externe Schnittstelle der ZSS (d.h. das Internet) realisiert. Wird die Kommunikation dagegen aus der inneren Sicherheitsschicht der ZSS initiiert, so gelten die in Abschnitt 1.3.1 dargelegten Kommunikationsregeln.

## 1.5 Verschlüsselte Speicherung der Daten

Im gesamten Verfahren sind personenbezogene Daten zu keiner Zeit unverschlüsselt auf Datenträgern zu speichern. Nach dem „Entfernen“ der Transport-Verschlüsselung sowie der Durchführung von logischen und fachlichen Prüfungen werden die Daten mit einem hybriden Verschlüsselungsverfahren (dynamischer Session-Key, der mit einem festen Datenbank-Hauptschlüssel verschlüsselt wird) verschlüsselt und im zentralen Datenbanksystem gespeichert.

Als Verschlüsselungsalgorithmen werden innerhalb der ZSS nur starke Algorithmen (z.B. AES 256 Bit) verwendet.

### 1.5.1 Hardware Security Modul (HSM)

Innerhalb der ZSS kommt ein Hardware-Security-Modul zum Einsatz. Innerhalb dieses Moduls werden die Datenbank-Hauptschlüssel gespeichert, die letzten Endes zur Ver- bzw. Entschlüsselung der Nutzdaten vor deren Speicherung in der zentralen Datenbank verwendet werden.

Der Zugriff auf diese Schlüsselinformationen ist auf dedizierte Hard- und Softwarekomponenten beschränkt, so dass eine unberechtigte Nutzung der Schlüssel ausgeschlossen werden kann. Die Verwaltung der HSM-Komponente ist nur im Vier-Augen-Prinzip möglich; im Umfeld der ZSS erfolgt hierfür eine Gewaltentrennung zwischen dem Betreiber des HSM sowie deren Eigentümer BfDI.

## 1.6 Datenschutz und Datensicherheit

Im ELENA-Verfahren werden personenbezogene Daten erfasst und gespeichert, auf deren Schutz und Sicherheit besonders hoher Wert gelegt wird. Zum Erreichen dieses Anspruchs sind bereits bei der Konzeption des Verfahrens die besonderen datenschutzrechtlichen Vorgaben des sechsten Abschnitts aus dem SGB IV und den allgemeinen Regelungen aus dem SGB X bzw. des BDSG und weitere sicherheitstechnische Festlegungen nach den Vorgaben des BSI formuliert und bei der Entwicklung der Verfahrensprozesse und Applikationssysteme berücksichtigt. Darüber hinaus wurden datenschutzrechtliche Eckpunkte durch das BMWi (**Anlage 4**, Schreiben des BMWi) formuliert, die ebenfalls bei der Realisierung berücksichtigt sind.

## **1.6.1 Übergreifend gültige Aspekte**

### **1.6.1.1 Trennung des Verfahrens in RFV und ZSS (Eckpunktekatalog Punkt 8)**

- o Nach § 96 Absatz 1 SGB IV ist die ZSS bei der DSRV eingerichtet.
- o Die ITSG nimmt die Aufgaben der RFV wahr (§ 96 Absatz 2 SGB IV).
- o Die Datenverarbeitungssysteme der ZSS und der RFV sind voneinander getrennt.  
Die Trennung ist auf räumlicher, organisatorischer, technischer und personeller Ebene eingehalten (§ 96 Absatz 4 SGB IV).

### **1.6.1.2 Zuordnung von Versicherungs- bzw. Verfahrensnummer zu vID/ZID nur in der RFV (Eckpunktekatalog Punkt 20)**

Es ist ausschließlich Aufgabe der RFV, die Versicherungsnummer bzw. die Verfahrensnummer mit der vID/ZID eines Teilnehmers oder seines Vertreters zu verbinden und zu speichern (§ 100 Absatz 1 Ziffer 3 SGB IV).

### **1.6.1.3 Kein Zugriff von Stellen, die nicht mit den Aufgaben des Anwendungsbereichs § 95 Absatz 1 SGB IV betraut sind (Eckpunktekatalog Punkt 15)**


Eine Übermittlung, Nutzung oder Beschlagnahme von Daten nach anderen Rechtsvorschriften ist unzulässig. Ein Zugriff von Sicherheitsbehörden, Steuerbehörden, Zoll etc. ist deshalb nicht gestattet (§§ 96 Absatz 3, 99 Absatz 6, 102 Absatz 4 SGB IV).

### **1.6.1.4 Zweckbindung der Meldedaten (Eckpunktekatalog Punkt 16)**

Die ZSS und RFV dürfen die Daten ausschließlich zur Erfüllung der im ELENA-Verfahrensgesetz formulierten Aufgaben nutzen. Eine darüber hinaus gehende Nutzung, z.B. für die Bildung eines Arbeitnehmer- oder Arbeitgeberregisters, ist nicht statthaft (§§ 99 Absatz 1, 100 Absatz 2 SGB IV).

### **1.6.1.5 Kein Outsourcing der durch das ELENA-Verfahrensgesetz formulierten Aufgaben**

Die Übertragung der Datenverarbeitung im Auftrag ist für ZSS und RFV unzulässig (§ 96 Absatz 3 SGB IV).

	<b>ELENA</b> <b>Verfahrensbeschreibung</b>	Seite: 21 Stand: <b>01.01.2010</b> Version: <b>1.0</b>
---	---	--

## **1.6.2 Datenschutz und Datensicherheit bei der RFV**

### **1.6.2.1 Sicherheitskonzeption des Betriebs nach BSI-Standard**

Das Sicherheitskonzept wird gemäß den BSI Standards 100-1, 100-2 und 100-3 erstellt.

### **1.6.2.2 Technische Aufteilung innerhalb der RFV**

Eine technische Aufteilung der RFV-Systeme zur Annahme der Anmeldungen (System mit Internet-Zugang) in eine innere (ISS) und äußere Sicherheitsschicht (ÄSS) mit jeweils physikalischen Trennmöglichkeiten und Überwachungsmechanismen ist erforderlich.

Das System zur verfahrensinternen Kommunikation („ZSS-Server“) besitzt keine Verbindung zum Internet und ist ausschließlich über ein abgesichertes virtuelles privates Netzwerk (VPN) in einer dedizierten Standleitung an die ZSS angeschlossen. Daher ist bei diesem System keine Trennung in ISS und ÄSS notwendig, der ZSS-Server selbst wird der inneren Sicherheitsschicht zugeordnet.

Eine Verschlüsselung der zentralen Datenbank ist nicht notwendig.

### **1.6.2.3 Dedizierte Hardware-Systeme**

Alle Systeme in der RFV sind dediziert, d. h. nur für ihre jeweilige Aufgabe im ELENA-Verfahren vorhanden. Die Systeme nehmen keine darüber hinaus gehenden Aufgaben wahr.

### **1.6.2.4 Hochverfügbarkeitslösungen**

Zur Sicherstellung des Grundwertes der hohen Verfügbarkeit werden Hochverfügbarkeitslösungen eingesetzt.

### **1.6.2.5 Implementierung von Intrusion Detection/Prevention Methoden**

Zur Überprüfung und Sicherstellung der „Fließrichtung“ von Daten werden, sobald eine direkte Verbindung zum Internet besteht, IDS/IPS Systeme eingesetzt.

### **1.6.2.6 Notfall- und Katastrophenkonzepte**

Zur Sicherstellung des Grundwertes der hohen Verfügbarkeit in einem Not- bzw. Katastrophenfall werden redundante Systeme bereitgestellt, welche die Funktionsfähigkeit der RFV sicherstellen.

### **1.6.2.7 Eigene und unabhängige Entwicklungs-, Test- und Produktionsumgebung**

Zur Sicherstellung der Grundwerte Verfügbarkeit und Integrität wird für den Bereich Entwicklung, Test und Produktion jeweils eine eigene Umgebung mit definierten Übernahmeprozessen bereitgestellt.

### **1.6.2.8 Vier-Augen-Prinzip bei kritischen Prozessen**

Administrative oder organisatorische Tätigkeiten in besonders kritischen Bereichen werden durch das Vier-Augen-Prinzip zusätzlich abgesichert (z. B. Firewallkonfigurationen).

### **1.6.3 Keine Einschränkung bei den verwendeten Signaturkarten (Eckpunktekatalog Punkt 12)**

Es können beliebig viele Signaturkarten pro Teilnehmer in das Verfahren eingebracht werden, sofern sie nach dem Signaturgesetz zugelassen sind, kein Pseudonym im Signaturzertifikat enthalten und eine Schnittstelle besitzen, mit der sie über das eCard-API Framework<sup>1</sup> angesprochen werden können.

### **1.6.4 Datenschutz und Datensicherheit bei der ZSS**

#### **1.6.4.1 Sicherheitskonzeption des Betriebs nach BSI-Standard**

Das Sicherheitskonzept der ZSS wird gemäß den BSI-Standards 100-1, 100-2 und 100-3 erstellt.

#### **1.6.4.2 Umfassende Trennung von ZSS und DSRV (Eckpunktekatalog Punkt 9)**

Bei der DSRV ist nach § 96 Absatz 1 SGB IV eine räumlich, organisatorisch und personell getrennte ZSS eingerichtet, welche die nach § 97 Absatz 1 SGB IV, übermittelten Daten speichert.

#### **1.6.4.3 Trennung der Verfahren innerhalb der ZSS (Eckpunktekatalog Punkt 3)**

Die technische Aufteilung der ZSS in einen meldenden (AG) und einen abrufenden Zweig (AS) und eine innere (ISS) und äußere Sicherheitsschicht (ÄSS) mit jeweils physikalischen Trennmöglichkeiten und Überwachungsmechanismen ist erforderlich.

---

<sup>1</sup> In Anlage 4 beschrieben

#### **1.6.4.4 Dedizierte Hardware-Systeme**

Alle Systeme in der ZSS sind dediziert, d. h. nur für ihre jeweilige Aufgabe im ELENA-Verfahren vorhanden. Die Systeme nehmen keine darüber hinaus gehenden Aufgaben wahr.

#### **1.6.4.5 Hochverfügbarkeitslösungen**

Zur Sicherstellung des Grundwertes der hohen Verfügbarkeit werden Hochverfügbarkeitslösungen eingesetzt.

#### **1.6.4.6 Implementierung von Intrusion Detection/Prevention Methoden**

Zur Überprüfung und Sicherstellung der „Fließrichtung“ der Datensätze vom meldenden Zweig schreibend in die zentrale Datenbank bzw. vom abrufendem Zweig lesend aus der zentralen Datenbank wird – wo sinnvoll möglich – ein IDS (Intrusion Detection System) bzw. ein IPS (Intrusion Prevention System) eingesetzt.

#### **1.6.4.7 Notfall- und Katastrophenkonzepte**

Zur Sicherstellung des Grundwertes der hohen Verfügbarkeit in einem Not- bzw. Katastrophenfall werden redundante Systeme bereitgestellt, welche die Funktionsfähigkeit der ZSS sicherstellen.

#### **1.6.4.8 Eigene und unabhängige Entwicklungs-/Test- und Produktionsumgebung**


Zur Sicherstellung der Grundwerte Verfügbarkeit und Integrität wird für den Bereich Entwicklung/Test und Produktion jeweils eine eigene Umgebung mit definierten Übernahmeprozessen bereitgestellt.

#### **1.6.4.9 Vier-Augen-Prinzip bei kritischen Prozessen**

Administrative oder organisatorische Tätigkeiten in besonders kritischen Bereichen werden durch das Vier-Augen-Prinzip zusätzlich abgesichert (z. B. Firewallkonfigurationen).

#### **1.6.4.10 Verschlüsselung der Transportwege der Meldedaten (Eckpunktekatalog Punkt 1)**

Die Übermittlung der Meldedaten hat nach § 28a Absatz 1 SGB IV durch gesicherte und verschlüsselte Datenübertragung zu erfolgen. Nachdem auch die ÄSS a priori als nicht sicher einzustufen ist, findet die Entschlüsselung der gemeldeten Datensätze zur Ablage in

	<b>ELENA</b> <b>Verfahrensbeschreibung</b>	Seite: 24 Stand: <b>01.01.2010</b> Version: <b>1.0</b>
---	---	--

der Zentralen Datenbank ausschließlich in der ISS-AG statt. Nur in der ISS-AS erfolgt das Auslesen, Entschlüsseln und Aufarbeiten der angefragten Datenfelder und die Neuverschlüsselung zur Übertragung an die abrufende Stelle.

#### **1.6.4.11 Verschlüsselung der Datensätze in der zentralen Datenbank (Eckpunktekatalog Punkt 2)**

Die gemeldeten Datensätze der Teilnehmer sind verschlüsselt in der Zentralen Datenbank abgelegt. Dazu werden die einzelnen Datenfelder eines Datensatzes mit einem Sitzungsschlüssel verschlüsselt und in die Tabelle(n) der zentralen Datenbank geschrieben. Der Sitzungsschlüssel wird wiederum mit dem Datenbank-Hauptschlüssel verschlüsselt und mit dem entsprechenden Datensatz zusammen abgelegt.

#### **1.6.4.12 BfDI bei Master-Key Szenario (Eckpunktekatalog Punkt 13)**

Der Datenbank-Hauptschlüssel (Master-Key) wird durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verwaltet (§ 99 Absatz 3 Satz 2 SGB IV); das bedeutet eine organisatorische und rechtliche Trennung zwischen der ZSS und der für den Master-Key verantwortlichen Stelle.

#### **1.6.4.13 Speicherung der Datensätze nur unter Ordnungsmerkmal VID/ZID (Eckpunktekatalog Punkt 6)**

Die Daten dürfen ausschließlich unter der Zertifikatsidentitätsnummer (ZID) oder der vorläufigen Identitätsnummer (VID) gespeichert werden (§ 99 Absatz 3 SGB IV).

#### **1.6.4.14 Löschen der Datensätze bei Fristablauf (Eckpunktekatalog Punkt 11)**

Die ZSS löscht die gespeicherten Daten automatisch, soweit die Ansprüche, für deren Geltendmachung sie nach den in § 95 Absatz 1 SGB IV genannten Gesetzen erforderlich sind, erloschen sind, spätestens nach fünf Jahren (§ 99 Absatz 4 SGB IV).

#### **1.6.4.15 Abruf nur durch zugelassene abrufende Stellen (Eckpunktekatalog Punkt 17)**

Der Datenabruf darf nur im Einvernehmen mit der RFV und ZSS durch berechnete, zugelassene, abrufende Stellen bzw. deren angemeldete Mitarbeiter erfolgen (§ 99 Absatz 7 SGB IV). Einzige Ausnahme ist die Selbstauskunft nach § 103 Absatz 4 SGB IV.



#### **1.6.4.16 Begrenzung des Datenabrufs (Eckpunktekatalog Punkt 14)**

Der Teilnehmer hat das Recht, sein Einverständnis zum Datenabruf jederzeit zu widerrufen und/oder zeitlich zu begrenzen. Das Einverständnis kann sich auch auf eine begrenzte Anzahl künftiger Abrufe beziehen. Der Abruf ist auf die Datensatzteile, die für die Aufgabenerfüllung erforderlich sind, zu begrenzen (§§ 103 Absatz 1, 101 Absatz 1 Nr. 2 SGB IV, § 3a BDSG - Datenvermeidung und Datensparsamkeit).

#### **1.6.4.17 „Zwei-Karten-Prinzip“ zum Abruf der Daten (Eckpunktekatalog Punkt 7)**

Die ZSS stellt sicher, dass Daten nur durch dazu Befugte abgerufen werden. Zur Prüfung dieser Abrufvoraussetzungen werden bei der ZSS die Abrufbefugnis der verantwortlichen Person sowie das Vorliegen des Einverständnisses des Teilnehmers mit dem Datenabruf durch die abrufende Stelle gespeichert. Beim Abruf prüft die ZSS die Authentizität des Bearbeiters in der abrufenden Stelle. Diese Kommunikation muss authentisiert und verschlüsselt erfolgen. Der Mitarbeiter oder die Mitarbeiterin der abrufenden Stelle weist sich gegenüber der ZSS durch ein registriertes Zertifikat aus und belegt dadurch seine oder ihre Abrufberechtigung. Gleiches gilt für den Abrufagenten (§ 99 Absatz 3 SGB IV).

#### **1.6.4.18 Einverständniserklärung des Teilnehmers mit qualifizierter Signatur (Eckpunktekatalog Punkt 4)**

Ein Abruf der bei der ZSS gespeicherten Daten ist nur zulässig, wenn der Teilnehmer oder dessen Vertreter mit seiner qualifizierten elektronischen Signatur sein Einverständnis erklärt hat (§ 103 Absatz 1 SGB IV).

#### **1.6.4.19 Einverständniserklärung durch bevollmächtigte Personen (Eckpunktekatalog Punkt 5)**

Der Vertreter eines Teilnehmers hat sich zusätzlich zum Verfahren anzumelden. Bei der Anmeldung zum Verfahren ist der Nachweis des gesetzlichen Vertretungsrechtes zu führen. Dieses muss zum Zeitpunkt der Einverständniserklärung für die vertretene Person noch bestehen (§§ 98 Absatz 3, 103 Absatz 1 SGB IV).

#### **1.6.4.20 Protokollierung der Datenbanktransaktionen**

#### **Protokollierung der Arbeitgebermeldungen (Eckpunktekatalog Punkt 18)**

In der ZSS wird der Eingang der Meldungen des Arbeitgebers protokolliert. Die Protokollierung umfasst nach § 99 Absatz 2 SGB IV:

- den Eingangszeitpunkt der Übermittlung
- den Monat für den die Meldung erfolgt
- die Versicherungs- oder Verfahrensnummer des Teilnehmers
- die Betriebsnummer des Beschäftigungsbetriebs

### **Protokollierung der Datenabrufe (Eckpunktekatalog Punkt 18)**

Die ZSS protokolliert die Datenabrufe. Die Protokollierung umfasst nach § 101 Absatz 2 SGB IV mindestens:

- den Abrufzeitpunkt
- die abrufende verantwortliche Person, bei Verwendung eines Abrufagenten auch die weiterverarbeitende Person
- die Zertifikatsidentitätsnummer zum abgerufenen Datensatz
- den Namen oder die Betriebsnummer der abrufenden Stelle

#### **1.6.4.21 Speicherung der Einverständniserklärungen (Eckpunktekatalog Punkt 19)**

Die für den Nachweis eines berechtigten Abrufes notwendige Einverständniserklärung ist mit der gleichen Frist wie die Protokollierung des Abrufs zu speichern.

### **1.6.5 Datenschutz und Datensicherheit bei den abrufenden Stellen**

Nach § 99 Absatz 7 Satz 4 SGB IV prüft die ZSS vor Zulassung einer abrufenden Stellen, ob die technischen und datenschutzrechtlichen Voraussetzungen für die Teilnahme am ELENA-Verfahren durch die abrufende Stelle gewährleistet sind. Hier ist ein Sicherheitskonzept von der ZSS, für die Anbindung der abrufenden Stellen, vorzugeben.

#### **1.6.5.1 Zweckbindung des Datenabrufs (Eckpunktekatalog Punkt 10)**

Die abgerufenen Daten dürfen nur zur Erstellung der im sechsten Abschnitt des SGB IV erfassten Nachweise genutzt werden. Ein entsprechender Antrag und eine gültige Einverständniserklärung müssen dabei vorliegen. Ohne Antrag erfolgt kein Datenabruf. Eine Ausnahme stellt hier die Selbstauskunft dar, da bei der Selbstauskunft nur ein Antrag zur Selbstauskunft vorliegt und somit nicht direkt ein Zweck verfolgt wird (§ 102 Absatz 4 SGB IV).

## 2 Verfahrens- und Prozessbeteiligte und deren Aufgaben

In diesem Kapitel werden die fachlichen Gegebenheiten bei den einzelnen Beteiligten und deren Beziehungen untereinander näher beschrieben und definiert.

Dies erfolgt unter dem Gesichtspunkt,

- **Wer** tauscht
- **Was**
- **Warum** (aufgrund welcher gesetzlichen Norm)
- mit **Wem**
- **Wann**
- und **Wie** aus.

### 2.1 Aufgaben und Kommunikationsbeziehungen der Verfahrensbeteiligten

#### 2.1.1 Arbeitgeber und Zentrale Speicherstelle


Bei der Kommunikation mit dem Arbeitgeber kommen Verfahren zum Einsatz, die in der Praxis bekannt und als sicher eingestuft sind. Es wird auf das DEÜV-Verfahren aufgesetzt.

##### 2.1.1.1 Meldung des Multifunktionalen Verdienstdatensatzes (MVDS) bei Gehaltsabrechnung

###### a) Rechtsgrundlage

Die Arbeitgeber haben nach § 97 Absatz 1 SGB IV

- für jeden Beschäftigten, Beamten, Richter oder Soldaten
- monatlich gleichzeitig mit der Entgeltabrechnung
- eine Meldung zu erstatten, welche die Daten enthält, die in die erfassten Nachweise aufzunehmen sind (§ 95 Absatz 1 SGB IV).

	<b>ELENA</b> <b>Verfahrensbeschreibung</b>	Seite: 28 Stand: <b>01.01.2010</b> Version: <b>1.0</b>
---	---	--

Es handelt sich dabei um folgende Bescheinigungen:

- Arbeitsbescheinigung gemäß § 312 SGB III
- Nebeneinkommensbescheinigung gemäß § 313 SGB III
- Auskunft über die Beschäftigung nach § 315 Absatz 3 SGB III
- Auskunft über den Arbeitsverdienst zum Wohngeldantrag nach § 23 Absatz 2 des Wohngeldgesetzes und
- Entgeltnachweise nach § 2 Absatz 7 Satz 4 und § 9 des Bundeselterngeld- und Elternzeitgesetzes

Nach § 99 SGB IV erhebt die ZSS die vom Arbeitgeber nach § 97 Absatz 1 SGB IV übermittelten Daten.

b) Schnittstelle:

Der Arbeitgeber erstellt aus der von ihm verwendeten Lohn- und Gehaltssoftware einen multifunktionalen Verdienstdatensatz (MVDS) für jeden seiner Arbeitnehmer. Diese Datensätze werden monatlich an die Zentrale Speicherstelle übermittelt. Die Übermittlung der Datensätze muss unverzüglich nach dem Ende des zu meldenden Monats erfolgen.

c) Datenübermittlung:

Für die Übermittlung des MVDS nach § 97 Absatz 1 SGB IV gilt die gesicherte und verschlüsselte Datenübertragung aus systemgeprüften Programmen oder mittels maschinell erstellter Ausfüllhilfen (§ 28a Absatz 1 SGB IV). Die Übertragungswege sind in den Gemeinsame Grundsätze für die Erstattung der Meldungen der Arbeitgeber an die Zentrale Speicherstelle im Rahmen des Verfahrens des elektronischen Entgeltnachweises nach § 28b Absatz 6 SGB IV geregelt. Nach Ziffer 6.2 gelten für die Übertragung zur ZSS die Richtlinien für den Datenaustausch (jetzt Richtlinien für den Datenaustausch im Gesundheits- und Sozialwesen). Diese sind unter dem Menüpunkt Grundlagen auf [www.gkv-ag.de](http://www.gkv-ag.de) zu finden.

Die einzelnen MVDS werden zu einer Datei zusammengefasst, die zusammen mit einem Auftragsatz an die Zentrale Speicherstelle übermittelt wird. Jede Datei beginnt mit einem Vorlaufsatz (VOSZ) und endet mit einem Nachlaufsatz (NCSZ). Zwischen dem Vorlaufsatz und dem Nachlaufsatz liegen die Datensätze und Datenbausteine. Nach dem Vorlaufsatz

sind der Datensatz Kommunikation (DSKO) und die einzelnen MVDS zu liefern. Es dürfen bis zu 2.000 MVDS in einer Datei per E-Mail und bis zu 20.000 MVDS per http/https unter Verwendung von eXTra übermittelt werden.

Die Datei selbst wird verschlüsselt und technisch signiert. Zur Verschlüsselung wird der öffentliche Schlüssel der Zentralen Speicherstelle benutzt, der dem Arbeitgeber in der Annahmestellendatei vom Arbeitgeber-Trustcenter zur Verfügung gestellt wurde.

Der Aufbau der Datensätze und Datenbausteine hinsichtlich der Plausibilitäts- bzw. Kernprüfung ist in der **Anlage 5** beschrieben. Neben der **Anlage 5** sind auch eine **Anlage 5a** und **Anlage 5b** vorgesehen. In der **Anlage 5a** werden die Hinweise beschrieben, die die ZSS an den Arbeitgeber sendet. Die **Anlage 5b** enthält die satzbezogenen Fehler (die nicht in die Anlage 5 enthalten sind) und ggf. auch Sendungsprüfungen.

Als weitere **Anlage 6** sind die Erläuterungen zu deren fachlichem Inhalt beigelegt. Im Mittelpunkt dieser Anlage steht dabei die Kommunikation mit den auf Empfängerseite zuständigen Behörden oder sonstigen öffentlich-rechtlichen Einrichtungen. Diese **Anlage 6** enthält detaillierte Beschreibungen und Informationen zu den einzelnen Feldern, um Softwarehäuser und Arbeitgeber bei Einrichtung und laufendem Betrieb des Verfahrens zu unterstützen. Das Dokument soll zudem als Aufhänger für die Klärung von Einzelfragen der Nutzer zum MVDS dienen.

Als weitere **Anlage 7** ist eine Zusammenstellung von Musterbeispielen beigelegt, die unterschiedliche Fallkonstellationen der ELENA-Meldungen (MVDS oder DSVV und Datenbausteine) in Verbindung mit den Entgeltabrechnungen schematisch darstellen. Das Schema der Fallbeispiele stellt keinerlei Formvorgabe dar und weist nur auszugsweise die für die Fallkonstellation wesentlichen Angaben aus. Ausschlaggebend für die ELENA-Meldungen sind ausschließlich - jeweils in der letztgültigen Fassung - die gesetzlichen Grundlagen, die „Gemeinsamen Grundsätze für die Erstattung der Meldungen der Arbeitgeber an die Zentrale Speicherstelle im Rahmen des Verfahrens des elektronischen Entgeltnachweises nach § 28b Absatz 6 SGB IV“ und die Verfahrensbeschreibungen.

d) Protokollierung bei Übermittlung beim Arbeitgeber

Die Zentrale Speicherstelle prüft die eingetroffenen Dateien und erstellt pro Datei eine Protokollmitteilung, die – je nach Verfahren - an den Arbeitgeber zurückgesandt oder ihm zur Abholung bereitgestellt wird.

Der Arbeitgeber hat nach § 97 Absatz 2 SGB IV den Versand der Meldung an die Zentrale Speicherstelle zu protokollieren. Die Protokollierung umfasst mindestens den Übermittlungszeitpunkt, den Meldemonat, die Versicherungs- oder Verfahrensnummer des Teilnehmers, die Betriebsnummer sowie die laufende Nummer der Datei. Die Protokolldaten sind nach zwei Jahren zu löschen, es sei denn, sie werden als Beweismittel in einem anhängigen Verwaltungs- und Gerichtsverfahren benötigt. In diesem Fall muss die Löschung unverzüglich nach Mitteilung über den Abschluss des Verfahrens erfolgen.

e) Korrektur bereits gemeldeter Datensätze

Sofern Daten nach der Übermittlung an die ZSS beim Arbeitgeber für einen Abrechnungszeitraum geändert werden, ist nach § 97 Absatz 5 SGB IV die Meldung für diesen Abrechnungszeitraum unverzüglich zu stornieren und unverzüglich eine erneute Meldung mit den geänderten Daten zu erstatten.

### **2.1.1.2 Rückmeldung der Verarbeitungsergebnisse je Sendung**

a) Rechtsgrundlage

Nach § 99 Absatz 2 Satz 1 SGB IV hat die Zentrale Speicherstelle die übermittelten Daten vom Arbeitgeber auf Schlüssigkeit und Vollständigkeit zu überprüfen. Der Eingang der Meldungen des Arbeitgebers ist zu protokollieren.

Die Protokollierung umfasst  
den Eingangszeitpunkt der Übermittlung  
den Monat für den die Meldung gilt  
die Versicherungs- oder Verfahrensnummer des Teilnehmers und  
die Betriebsnummer des Beschäftigungsbetriebes.

Nach § 99 Absatz 2 Satz 3 SGB IV i. V. m. § 97 Absatz 2 Satz 2 und 3 SGB IV sind Protokolldaten nach zwei Jahren zu löschen, es sei denn, sie werden als Beweismittel in einem anhängigen Verwaltungs- und Gerichtsverfahren benötigt. In diesem Fall muss die Löschung unverzüglich nach Mitteilung über den Abschluss des Verfahrens erfolgen.

**b) Schnittstellen**

Die Rückmeldung erfolgt abhängig vom Übermittlungsverfahren (eMail, eXTra, etc.).

**c) Datenübermittlung**

Für die Übermittlung von MVDS nach § 97 Absatz 1 SGB IV gilt die gesicherte und verschlüsselte Datenübertragung aus systemgeprüften Programmen oder mittels maschinell erstellter Ausfüllhilfen (§ 28a Absatz 1 SGB IV). Die Übertragungswege sind in den Gemeinsamen Grundsätzen für die Datenerfassung und Datenübermittlung zur Sozialversicherung nach § 28b Absatz 2 SGB IV geregelt. Soweit keine personenbezogenen Daten übermittelt werden, kann die Verschlüsselung entfallen.

**d) Aktivitäten beim Arbeitgeber**

Bei positiver Quittung waren die übermittelten Datensätze syntaktisch fehlerfrei und vollständig. Die semantische Prüfung hatte keine Fehler ergeben. Die positive Quittung bestätigt dies pro Datei.

Sind die Daten nicht schlüssig oder unvollständig oder erfolgt aus sonstigen Gründen keine Speicherung, ist der Arbeitgeber nach § 99 Absatz 2 Satz 4 SGB IV durch eine Fehlermeldung zu unterrichten. Enthalten ein oder mehrere übermittelte Datensätze Fehler, teilt der datensatzbezogene Fehlertext mit, wo syntaktische oder semantische Fehler vorhanden sind bzw. wo Daten fehlen. Der Arbeitgeber muss in den fehlerhaften Datensätzen die Unstimmigkeiten beseitigen und diese Datensätze erneut gemäß § 99 Absatz 2 Satz 6 unverzüglich senden. Die fehlerhaften Datensätze wurden nicht in der Zentralen Speicherstelle gespeichert.

Erhält der Arbeitgeber innerhalb von fünf Tagen nach Versand seiner E-Mail keine Mitteilung und ist im Serviceportal der ZSS kein aktueller Status dieser Meldung zu finden, hat der Arbeitgeber die komplette Sendung noch einmal zu versenden.

**2.1.1.3 Anforderung einer Versicherungsnummer / Verfahrensnummer****e) Rechtsgrundlage:**

Ist für einen Beschäftigten, Beamten, Richter oder Soldaten keine Versicherungsnummer nach § 147 SGB VI vorhanden oder zu vergeben, beantragt der Arbeitgeber nach § 97 Absatz 4 SGB IV mit der Meldung nach § 97 Absatz 1 SGB IV die Vergabe einer

Verfahrensnummer bei der Zentralen Speicherstelle unter Angabe der für die Vergabe der Verfahrensnummer erforderlichen Daten des Beschäftigten, Beamten, Richter oder Soldaten.

f) Schnittstellen:

Die Arbeitgeber melden den Datensatz Vergabe einer Versicherungs-/Verfahrensnummer (DSVV) mit den Datenbausteinen DBNA, DBGB und DBAN. Das Feld VSNR-VFNR im Datensatz DSVV bleibt dabei leer.

g) Datenübermittlung:

Für die Übermittlung des Datensatzes DSVV zur Ermittlung der Versicherungs-/Verfahrensnummer nach § 97 Absatz 4 SGB IV gilt die gesicherte und verschlüsselte Datenübertragung aus systemgeprüften Programmen oder mittels maschinell erstellter Ausfüllhilfen (§ 28a Absatz 1 SGB IV). Die Übertragungswege sind in den gemeinsamen Grundsätzen nach § 28b Absatz 2 SGB IV geregelt.

Die einzelnen Datensätze DSVV werden zu einer Datei (Vorlaufsatz, Datensatz DSKO, 1 bis n Datensätze DSVV, Nachlaufsatz) zusammengefasst, die zusammen mit einem Auftragsatz an die Zentrale Speicherstelle übermittelt werden. In dieser Datei dürfen keine Datensätze MVDS enthalten sein. Die Datei selbst wird verschlüsselt und technisch signiert. Zur Verschlüsselung wird der öffentliche Schlüssel der Zentralen Speicherstelle benutzt, der dem Arbeitgeber in der Annahmestellendatei vom Arbeitgeber-Trustcenter zur Verfügung gestellt wurde.

#### **2.1.1.4 Rückmeldung einer Versicherungsnummer / Verfahrensnummer**

a) Rechtsgrundlage:

Nach § 97 Absatz 4 Satz 4 SGB IV ist dem Arbeitgeber durch die ZSS unverzüglich die vergebene oder ermittelte Verfahrensnummer mitzuteilen. Dies kann auch elektronisch erfolgen.

b) Schnittstelle:

Vor dem Abgleich mit dem Stammsatzdatenbestand erfolgt eine Prüfung der gelieferten Adressdaten. Sind diese fehlerhaft, erfolgt eine Fehlermeldung mit dem Datensatz DSVV und dem Datenbaustein DBFE mit der entsprechenden Fehlernummer. Die Adressdaten sind



dann durch den Arbeitgeber zu prüfen und der korrigierte Datensatz DSVV ist erneut zu übermitteln.

Können die gelieferten Adressdaten durch das Prüfprogramm sicher korrigiert werden, erfolgt die Rückmeldung mit dem Datensatz DSVV und den zugehörigen Datenbausteinen sowie dem Datenbaustein DBFE mit einem entsprechenden Hinweis. Die korrigierten Adressdaten werden bei der Rückmeldung an den Arbeitgeber immer in den Datenbaustein DBAN eingetragen. Die veränderten Adressdaten können dann in die Bestandsdaten des Arbeitgebers übernommen werden.

Sofern für den Arbeitnehmer eindeutig eine Versicherungs- oder Verfahrensnummer im Stammsatzdatenbestand ermittelt wird, erfolgt eine positive Rückmeldung mit dem Datensatz DSVV und den zugehörigen Datenbausteinen DBNA, DBGB und DBAN. Dabei wird die aktuelle Versicherungs- oder Verfahrensnummer in das Feld VSNR-VFNR des Datensatzes DSVV eingetragen.

Wenn im Stammsatzdatenbestand keine Versicherungs- oder Verfahrensnummer vorhanden ist und es sich nicht um einen Beamten handelt, wird im ELENA-Verfahren keine Versicherungsnummer vergeben. In diesen Fällen erfolgt eine Fehlermeldung mit dem Datensatz DSVV und dem Datenbaustein DBFE mit der Bitte, die Vergabe einer Versicherungsnummer im DEÜV-Verfahren über die Einzugsstelle des Gesamtsozialversicherungsbeitrages einzuleiten, weil keine Versicherungsnummer im Stammsatzdatenbestand vorhanden ist.

Wenn im Stammsatzdatenbestand keine Versicherungs- oder Verfahrensnummer vorhanden ist und es sich um einen Beamten handelt, wird eine Verfahrensnummer vergeben. Die Rückmeldung erfolgt mit dem Datensatz DSVV und den zugehörigen Datenbausteinen DBNA, DBGB und DBAN. Dabei wird die neu vergebene Verfahrensnummer in das Feld VSNR-VFNR des DSVV eingetragen.

Kann im Stammsatzdatenbestand eine Versicherungs- oder Verfahrensnummer nicht eindeutig zugeordnet werden und es handelt sich nicht um einen Beamten, erfolgt die Rückmeldung des Datensatzes DSVV und den zugehörigen Datenbausteinen sowie dem Datenbaustein DBFE mit der Bitte, die Vergabe einer Versicherungsnummer im DEÜV-

Verfahren über die Einzugsstelle des Gesamtsozialversicherungsbeitrages einzuleiten, weil keine Versicherungsnummer eindeutig zugeordnet werden konnte.

Kann im Stammsatzdatenbestand eine Versicherungs- oder Verfahrensnummer nicht eindeutig zugeordnet werden und es handelt sich um einen Beamten, erfolgt zunächst die Rückmeldung des Datensatzes DSVV und den zugehörigen Datenbausteinen sowie dem Datenbaustein DBFE mit dem Hinweis, dass ein Prüffall bei der DSRV erzeugt wurde. Nach Klärung des Prüffalls durch die Sachbearbeitung der Rentenversicherungsträger erfolgt die Rückmeldung des ursprünglichen Datensatzes DSVV und den zugehörigen Datenbausteinen. Dabei wird entweder die aktuelle Versicherungs- oder Verfahrensnummer in das Feld VSNR-VFNR des Datensatzes DSVV eingetragen oder der Vergabeantrag aufgrund offensichtlich unplausibler personenbezogener Daten mit angehängtem Datenbaustein DBFE abgewiesen..

c) Datenübermittlung

Die Übertragungswege für die Rückmeldungen sind in den gemeinsamen Grundsätzen nach § 28b Absatz 2 SGB IV geregelt.

### **2.1.1.5 Statusabfrage AG (nur lesend)**

Der Arbeitgeber hat die Möglichkeit, über einen Statusserver bei der ZSS den Verarbeitungsstand seiner Meldungen nachzuvollziehen.

### **2.1.2 Zentrale Speicherstelle und Registratur Fachverfahren**

Die Registratur Fachverfahren wird im ELENA-Verfahren benötigt, um die Versicherungsnummer (VSNR) oder Verfahrensnummer eines Teilnehmers zu pseudonymisieren. Das erfolgt, indem die VSNR mit der Zertifikatsidentitätsnummer verknüpft wird. Ist noch keine Signaturkarte zum Verfahren angemeldet, erfolgt die Verknüpfung der Versicherungsnummer/Verfahrensnummer mit einer vorläufigen Identitätsnummer.

#### **2.1.2.1 Anforderung VID/ZID**

a) Rechtsgrundlage:

Bei Eingang eines MVDS prüft die Zentrale Speicherstelle gemäß § 99 Absatz 3 Satz 1 SGB IV durch eine Abfrage bei der Registratur Fachverfahren die Möglichkeit der Zuordnung zu

einer Zertifikatsidentitätsnummer (ZID) oder vorläufigen Identitätsnummer (vID), da die durch den Arbeitgeber übermittelten Daten ausschließlich unter der ZID oder vID gespeichert werden dürfen (§ 99 Absatz 3 Satz 2 SGB IV).

b) Schnittstellen:

Die ZSS meldet den Datensatz MVDS mit den Datenbausteinen DBNA, DBGB und DBAN an die RFV. Die restlichen Datenbausteine des MVDS werden bei der Anfrage nicht an die RFV übermittelt.

c) Datenübermittlung:

Die Übermittlung erfolgt immer elektronisch über die definierte Schnittstelle zwischen dem ISS-AG System der Zentralen Speicherstelle und dem ZSS-Server der Registratur Fachverfahren (siehe Abschnitt 4.3.1).

### 2.1.2.2 Rückmeldung vID/ZID

a) Rechtsgrundlage:

Die Registratur Fachverfahren hat gemäß § 100 Absatz 1 Nr. 3 SGB IV die Aufgabe, die Zertifikatsidentitätsnummer oder vorläufige Identitätsnummer des Teilnehmers beziehungsweise des gesetzlichen Vertreters mit der Versicherungs- oder Verfahrensnummer des Teilnehmers zu verbinden und zu speichern und diese der Zentralen Speicherstelle auf Anfrage zu übermitteln (§ 100 Absatz 1 Nr. 6 SGB IV).

b) Schnittstellen:

Die RFV sendet grundsätzlich den ursprünglich von der ZSS übermittelten Basisdatensatz MVDS ohne die Datenbausteine DBNA, DBGB und DBAN an die ZSS zurück.

Sofern die Versicherungs- oder Verfahrensnummer im Stammsatzbestand vorhanden ist und eindeutig einer Person zugeordnet werden konnte, erfolgt die Rückmeldung aller zu einer Person bei der RFV gespeicherten vID/ZID mit angehängtem Datenbaustein DBID<sup>2</sup>,

Ist die Versicherungs- oder Verfahrensnummer ungültig oder nicht vorhanden, wird der von der DSRV um einen oder mehrere Datenbausteine DBFE ergänzte MVDS von der RFV an die ZSS weitergeleitet.

---

<sup>2</sup> Definition des DBID siehe Anlage 3b

c) Datenübermittlung:

Die Übermittlung erfolgt immer elektronisch über die definierte Schnittstelle zwischen dem ISS-AG System der Zentralen Speicherstelle und dem ZSS-Server der Registratur Fachverfahren (siehe Abschnitt 4.3.1).

### **2.1.3 RFV und DSRV**

#### **2.1.3.1 Prüfung der Versicherungs- oder Verfahrensnummer nach Meldung des MVDS**

a) Rechtsgrundlage:

In analoger Anwendung des § 100 Absatz 4 SGB IV wird bereits bei der Übermittlung des MVDS ein Abgleich mit dem Stammdatensatzbestand der Datenstelle der Träger der Rentenversicherung durchgeführt, bevor die Verknüpfung zwischen der Versicherungsnummer oder Verfahrensnummer und der ZID oder VID erfolgt.

b) Schnittstellen:

Die Anfrage der RFV an die DSRV erfolgt mit dem Datensatz MVDS und den Datenbausteinen DBNA, DBGB und DBAN. Es wird geprüft, ob die mit dem MVDS gelieferte Versicherungs- oder Verfahrensnummer zum Stammdatensatz passt.

c) Datenübertragung:

Die Übermittlung erfolgt immer elektronisch über die definierte Schnittstelle zwischen dem System der DSRV und dem ZSS-Server der Registratur Fachverfahren (siehe Abschnitt xx).

#### **2.1.3.2 Rückmeldung nach Prüfung der Versicherungsnummer**

a) Rechtsgrundlage:

In analoger Anwendung des § 100 Absatz 4 SGB IV wird bereits bei der Übermittlung des MVDS ein Abgleich mit dem Stammdatensatzbestand der Datenstelle der Träger der Rentenversicherung durchgeführt bevor die Verknüpfung zwischen der Versicherungsnummer und der ZID oder VID erfolgt.

b) Schnittstellen:

Die Rückmeldung der Versicherungsnummer durch die DSRV an die RFV erfolgt grundsätzlich mit dem Datensatz MVDS und den Datenbausteinen DBNA, DBGB und DBAN.

~ Bei vorliegender Personenidentität werden die aktuelle Versicherungsnummer in den Datenbaustein DBVR und ggf. zugehörige stillgelegte Versicherungsnummern in den Datenbaustein DBST eingetragen<sup>3</sup>.

~ Sofern die Versicherungsnummer nicht mit den gelieferten Daten übereinstimmt, erfolgt eine Fehlermeldung mit dem Datenbaustein DBFE.

c) Datenübertragung:

Die Übermittlung erfolgt immer elektronisch über die definierte Schnittstelle zwischen dem System der DSRV und dem ZSS-Server der Registratur Fachverfahren (siehe Abschnitt 4.3.1).

### **2.1.3.3 Anmeldung eines Teilnehmers**

### **2.1.4 Teilnehmer und ZSS**

#### **2.1.4.1 Widerruf Einverständnis**

### **2.1.5 Abrufende Stelle und ZSS**

### **2.1.6 ZSS und DSRV**

#### **2.1.6.1 Anforderung einer Versicherungsnummer / Verfahrensnummer**

a) Rechtsgrundlage:

---

<sup>3</sup> Beide Datenbausteine sind im Anhang XXX beschrieben

Für Beschäftigte, Beamte, Richter und Soldaten, für die keine Versicherungsnummer nach § 147 SGB VI vorhanden oder zu vergeben ist, hat die ZSS den Antrag des Arbeitgebers zur Vergabe einer Verfahrensnummer an die DSRV weiterzuleiten (§ 97 Absatz 4 SGB IV).

b) Schnittstelle:

Der von den Arbeitgebern gemeldete Datensatz Vergabe einer Versicherungs-/Verfahrensnummer (DSVV) mit den Datenbausteinen DBNA, DBGB und DBAN wird an die DSRV weitergeleitet.

c) Datenübermittlung:

Die Übermittlung erfolgt immer elektronisch über die definierte Schnittstelle zwischen dem ISS-AG System der Zentralen Speicherstelle und dem eXtra-Server-ELENA der DSRV. Die technischen Einzelheiten der Datenübermittlung zwischen ZSS und DSRV sind durch eine Vereinbarung zu regeln.

### **2.1.6.2 Rückmeldung der Versicherungsnummer / Verfahrensnummer**

a) Rechtsgrundlage:

Für die Beschäftigten und die Arbeitgeber hat die DSRV in Anwendung des § 97 Absatz 4 SGB IV der ZSS die erforderliche Verfahrensnummer zur Verfügung zu stellen.

b) Schnittstelle :

Die Rückmeldung der DSRV an die ZSS erfolgt mit dem Datensatz DSVV und den zugehörigen Datenbausteinen DBNA, DBGB, DBAN und ggf. DBVR und DBFE in Abhängigkeit der vorliegenden Voraussetzungen. Diese und die entsprechenden Reaktionen der DSRV und der ZSS bei eindeutigen Feststellungen durch die DSRV sind nachfolgend abgebildet (die Behandlung der Fehler- und Prüffälle ist nicht Bestandteil der nachfolgenden Tabelle):

	Voraussetzungen			Reaktionen							
	VFNR vorhanden	VSNR vorhanden	Beamter	1	2	3	4	5	6	7	8
1	J	J	J	-	-	-	-	-	-	-	-
2	J	J	N	-	-	-	-	-	-	-	-
3	J	N	J					X			X
4	J	N	N	X				X	X		X
5	N	J	J					X			X
6	N	J	N					X			X
7	N	N	J		X		X			X	X
8	N	N	N			X					

### Reaktionen

- 1 DSRV aktiviert Verfahrensnummer (wird zur Versicherungsnummer)
- 2 DSRV vergibt eine Verfahrensnummer
- 3 DSRV meldet GDMQ = 24 im DBVR an die ZSS
- 4 DSRV meldet GDMQ = 21 im DBVR an die ZSS
- 5 DSRV meldet GDMQ = 02 im DBVR an die ZSS
- 6 Information des Teilnehmers durch die DSRV
- 7 Information des Teilnehmers durch die ZSS
- 8 DSRV meldet Nummer an ZSS und ZSS meldet Nummer an Arbeitgeber

Die aktuelle Versicherungs- oder Verfahrensnummer wird immer in das Feld VSNR-VFNR des Datensatzes DSVV eingetragen. Im Feld GDMQ des Datenbausteins DBVR ist zusätzlich zu kennzeichnen, ob es sich um die

- Rückmeldung einer Versicherungs- oder Verfahrensnummer (GDMQ 02),
- Rückmeldung einer neu vergebenen Verfahrensnummer (GDMQ 21),
- Rückmeldung eines Prüffalles bei einem Beamten (GDMQ 22),
- Rückmeldung eines Prüffalles bei einem Beschäftigten (GDMQ 23),

- die Rückmeldung bei einer nicht durchgeführten Versicherungsnummernvergabe (GDMQ 24),
- die Fehlerrückmeldung bei fehlerhaften Anschriftendaten (GDMQ 25) oder
- die Fehlerrückmeldung bei unplausiblen personenbezogenen Daten (GDMQ 26) handelt.



Für einen Nichtbeamten wird im ELENA-Verfahren keine Versicherungsnummer durch die DSRV vergeben.

Bei der Aktivierung einer Verfahrensnummer werden die üblichen Prozesse durch die DSRV angestoßen. Dazu gehört auch die Unterrichtung des Versicherten über die vergebene Versicherungsnummer durch Ausstellung eines Sozialversicherungsausweises.

Bei der Vergabe einer Verfahrensnummer wird der Teilnehmer durch die ZSS über die neu vergebene Verfahrensnummer informiert.

Bei einem Prüffall für einen Beamten wird die ZSS zunächst darüber informiert, dass ein Prüffall vorliegt. Nach Klärung des Prüffalles durch den Rentenversicherungsträger wird der ZSS entweder eine gültige Versicherungs- oder Verfahrensnummer oder bei offensichtlich unplausiblen personenbezogenen Daten zusätzlich der Datenbaustein DBFE übermittelt.

Bei einem Prüffall für einen Beschäftigten erfolgt keine Klärung durch die Rentenversicherungsträger.

Vor dem Abgleich mit dem Stammsatzdatenbestand erfolgt generell eine Prüfung der gelieferten Adressdaten. Bei fehlerhaften Adressdaten erfolgt die Rückmeldung des Datensatzes DSVV mit den Datenbausteinen DBNA, DBGB und DBAN und dem Datenbaustein DBFE an die ZSS.

Können die Adressdaten durch das Prüfprogramm sicher verändert werden, erfolgt die Rückmeldung des Datensatzes DSVV und den Datenbausteinen DBNA, DBGB, DBAN und DBVR sowie dem Datenbaustein DBFE mit einem entsprechenden Hinweis an die ZSS. Die korrigierten Adressdaten werden bei der Rückmeldung an die ZSS in den Datenbaustein DBAN eingetragen.

c) Datenübermittlung:

Die Übermittlung erfolgt immer elektronisch über die definierte Schnittstelle zwischen dem ISS-AG System der Zentralen Speicherstelle und dem eXtra-Server-ELENA der DSRV. Die technischen Einzelheiten der Datenübermittlung zwischen ZSS und DSRV sind durch eine Vereinbarung zu regeln.

## **2.1.7 ZSS und AG-Trustcenter**

### **2.1.7.1 Verifizieren Arbeitgeberschlüssel**

Die ZSS nimmt die monatliche Meldung eines Arbeitgebers an, sofern er ein entsprechendes Zertifikat vorweisen kann. Die Zertifikate werden der ZSS einmal täglich in Dateiform mit dem Dateinamen „gesamt.agv“ zur Verfügung gestellt, die alle gültigen Zertifikate aller zugelassenen Arbeitgeber in Deutschland enthält.

Sofern das Zertifikat eines Arbeitgebers in der „gesamt.agv“ enthalten ist, ist der Arbeitgeber für das ELENA-Verfahren zugelassen.

## **2.1.8 ZSS und Trustcenter**

### **2.1.8.1 Verifizieren der Zertifikatsdaten bei Abruf**

### **2.1.9 Abrufende Stelle und Trustcenter**

## **3 Verarbeitungsprozesse**

### **3.1 Verarbeitung eines MVDS**

#### **3.1.1 Meldung des MVDS bei Gehaltsabrechnung**

In der nachfolgenden Abbildung sind die wesentlichen Verarbeitungsprozesse grafisch dargestellt (Vorprüfung der Sendung, Entschlüsselung der Daten, Prüfung der Datensätze auf Vollständigkeit und Schlüssigkeit

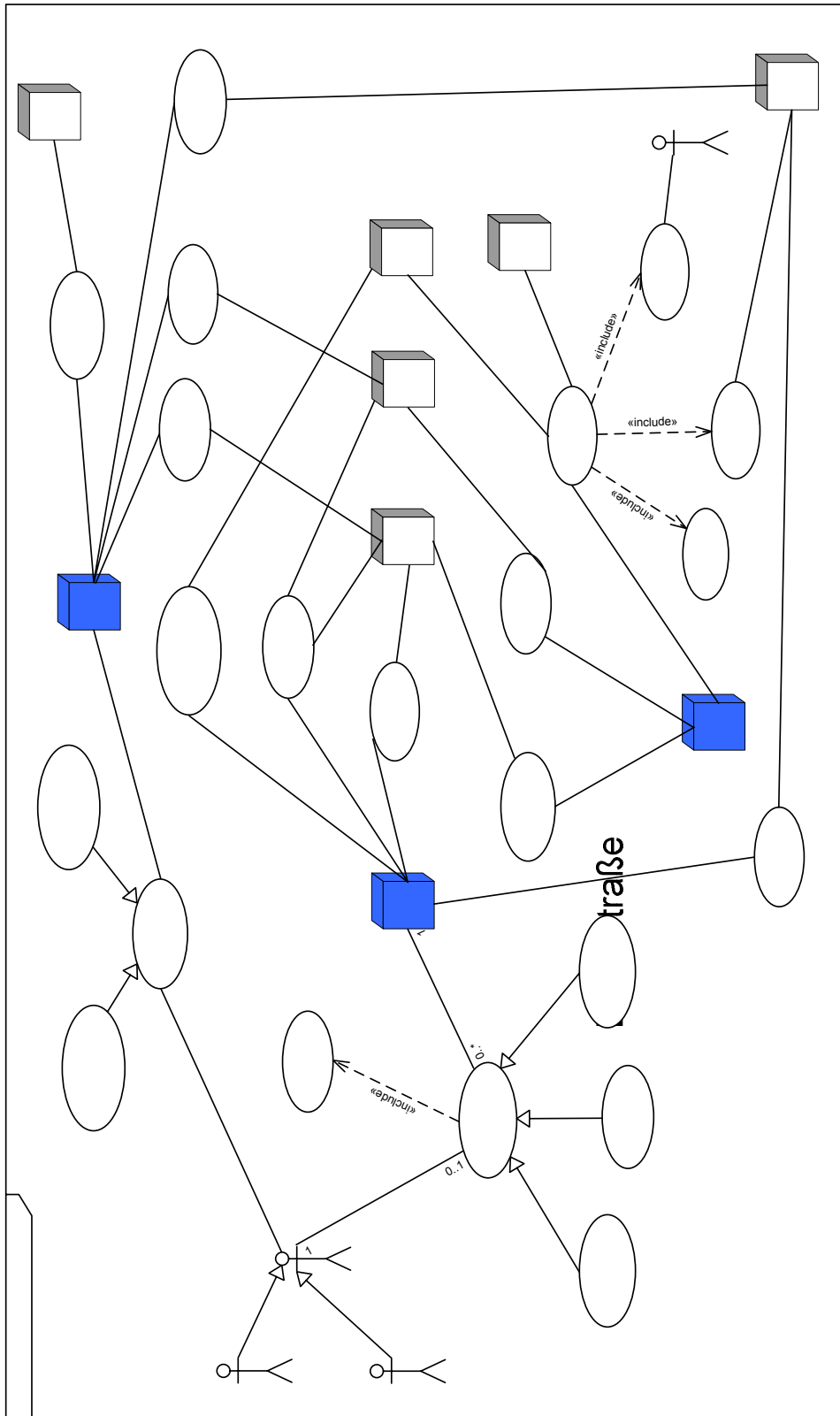


Abbildung 5: Verarbeitung eines MVDS

Dokumente für  
Druckstraße  
bereitstellen

Ausgangs-  
informationen  
abrufen

Kommunika-  
tionsparameter  
abrufen

### 3.2 Verarbeitung eines DSVV

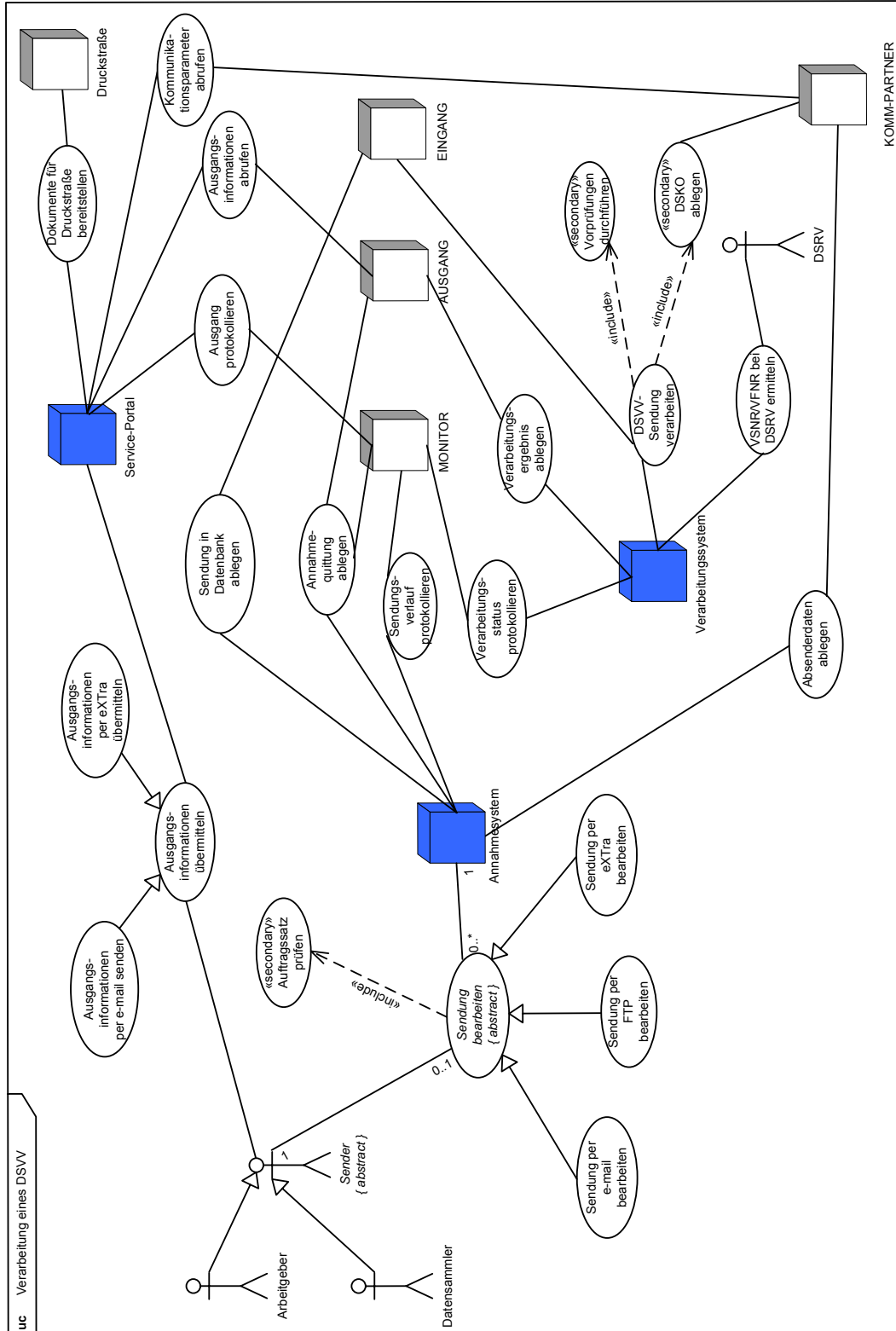
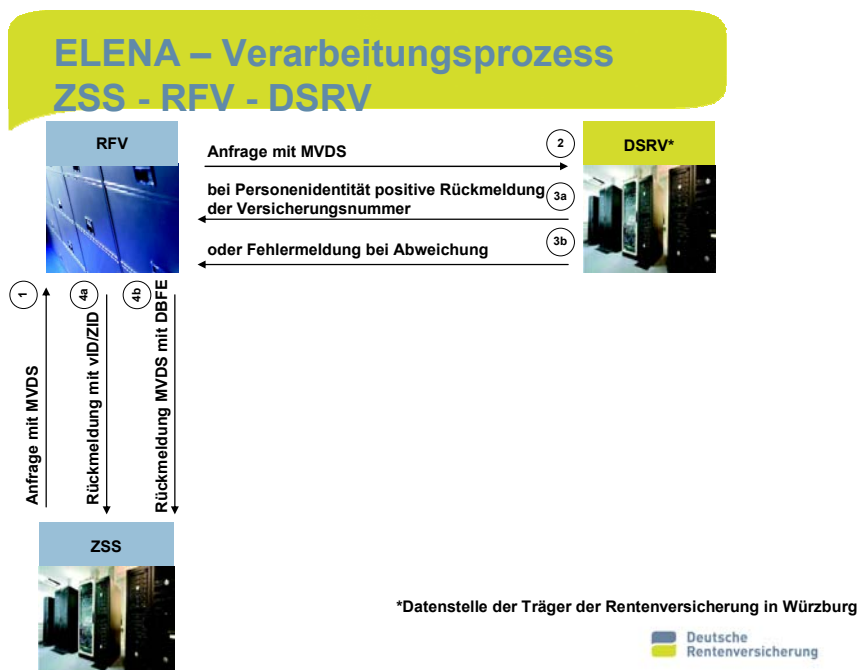


Abbildung 6: Verarbeitung eines DSVV

### Prüfung der Versicherungs- bzw. Verfahrensnummer nach Meldung des MVDS

Die DSRV prüft die Versicherungs- bzw. Verfahrensnummer des Arbeitnehmers auf Personenidentität. Sofern die gemeldete Versicherungs- bzw. Verfahrensnummer eindeutig zu der Person passt, meldet die DSRV die aktuell gültige und ggf. alle zugehörigen stillgelegten Versicherungs- bzw. Verfahrensnummern an die RFV zurück.

Weichen die persönlichen Daten im Stammsatzbestand von den Daten im MVDS ab oder ist die Versicherungs- bzw. Verfahrensnummer ungültig oder nicht im Stammsatzbestand vorhanden, erfolgt eine entsprechende Fehlerrückmeldung an die RFV (vgl. Abbildung).

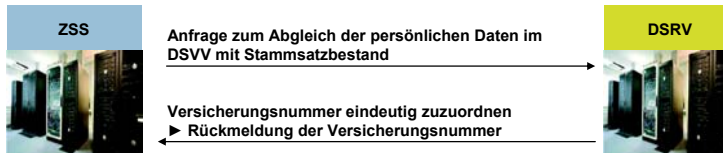


### Ermittlung einer Versicherungs- oder Verfahrensnummer und Vergabe einer Verfahrensnummer

Die DSRV prüft zunächst, ob mit den persönlichen Daten im DSVV eine Versicherungsnummer im Stammsatzbestand vorhanden ist. Folgende Möglichkeiten kommen in Betracht:

1. Kann eine Versicherungsnummer eindeutig zugeordnet werden, erfolgt die Rückmeldung der Versicherungsnummer an die ZSS (vgl. Abbildung).

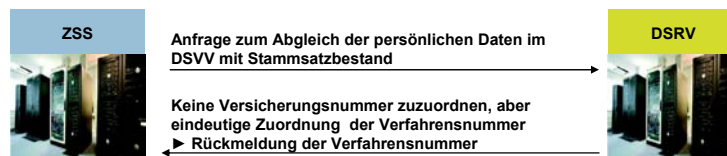
## ELENA - Verarbeitungsprozess ZSS - DSRV



**Abbildung 7: Verarbeitungsprozess ZSS - DSRV**

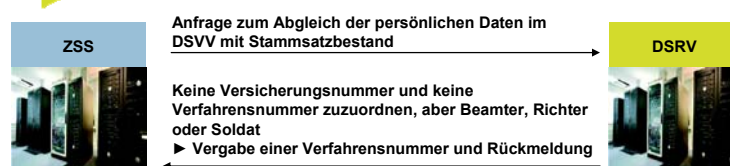
2. Kann eindeutig keine Versicherungsnummer zugeordnet werden, wird mit den persönlichen Daten nach einer Verfahrensnummer gesucht und
  - o kann eine Verfahrensnummer eindeutig zugeordnet werden, erfolgt die Rückmeldung der Verfahrensnummer an die ZSS (vgl. Abbildung)

## ELENA - Verarbeitungsprozess ZSS - DSRV



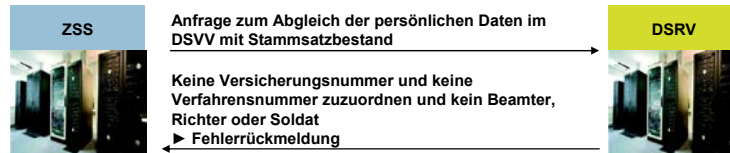
- o kann eindeutig keine Verfahrensnummer zugeordnet werden
  - und es handelt sich um einen Beamten, Richter oder Soldaten, so wird eine Verfahrensnummer durch die DSRV vergeben und an die ZSS zurückgemeldet. Die Verfahrensnummer beginnt immer mit der Bereichsnummer „01“ (vgl. Abbildung).

## ELENA - Verarbeitungsprozess ZSS - DSRV



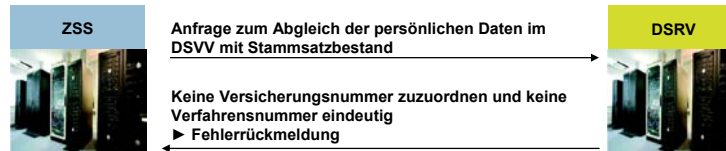
- und es handelt sich nicht um einen Beamten, Richter oder Soldaten, erfolgt eine Fehlerrückmeldung an die ZSS (vgl. Abbildung).

### ELENA - Verarbeitungsprozess ZSS - DSRV



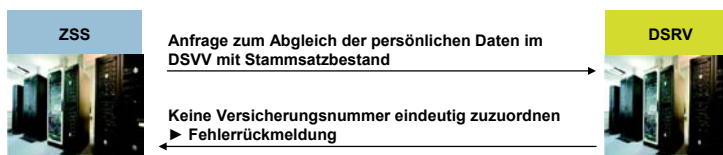
- kann eine Verfahrensnummer nicht eindeutig zugeordnet werden, erfolgt eine Fehlerrückmeldung an die ZSS (vgl. Abbildung).

### ELENA - Verarbeitungsprozess ZSS - DSRV



3. Kann eine Versicherungsnummer nicht eindeutig zugeordnet werden, erfolgt eine Fehlerrückmeldung an die ZSS (vgl. Abbildung).

### ELENA - Verarbeitungsprozess ZSS - DSRV



#### 3.2.1 Bekanntgabe einer vergebenen Verfahrensnummer an den Teilnehmer

Der Beamte, Richter oder Soldat wird gemäß § 97 Absatz 4 Satz 4 SGB IV über die Vergabe der Verfahrensnummer durch die DSRV schriftlich unterrichtet.



### **3.3 ZSS zu abrufenden Stellen**

### **3.4 ZSS mit RFV und DSRV**

#### **3.4.1 Prüfung der Versicherungs- bzw. Verfahrensnummer nach Meldung des MVDS**

Der Prozess kann dem folgenden Übersichtsdigramm entnommen werden:

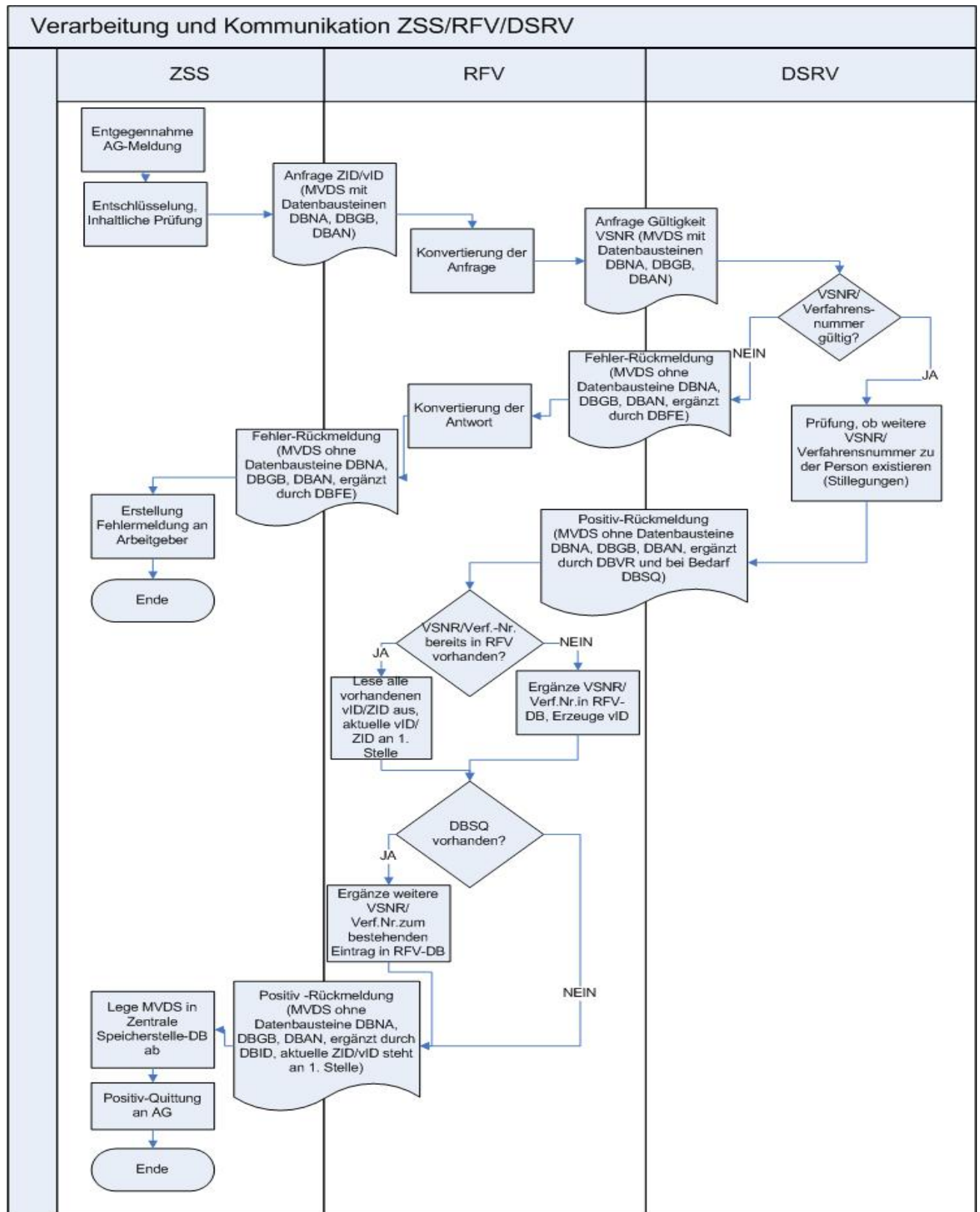


Abbildung 8 Übersicht über den Prozess

### 3.4.1.1 DSRV Kommunikationszustände

RFV liefert Anfragen an den eXTra Server der DSRV

eXTra Server DSRV prüft Schemadatei

Statusabelle D01 Schema Anfrage fehlerhaft

Statusabelle D09 Fehler beim Aufbau der Response

Schemadatei wird entpackt

Statusabelle D02 Datenteil (Body) konnte nicht gefunden werden

MVDS für Connector aufbereiten

Statusabelle D03 MVDS Aufbau im Datenpaket ungültig (xxxxx Satzähler)

Connector DSRV aufrufen

Statusabelle D04 DSRV Connector konnte nicht aufgerufen werden

Statusabelle D08 Technischer Fehler DSRV Connecotr

Statusabelle D10 Timeout bei der Anfrage über den DSRV Connector

CICS IBM Host Transaktion xxxx aufrufen

Statusabelle D05 CICS IBM Host Transaktion xxxx konnte nicht aufrufen

IBM Host Doppelvergabeverdachtsprüfung

Statusabelle T01 Lesefehler im SMSZ-Bestand

Statusabelle T02 Lesefehler im Perso-Bestand

Statusabelle T04 Lesefehler im Alpha-Suchbestand

Statusabelle T05 DSRV Doppelvergabeverdachtsprüfung, fehlerhafter

Anfrageschlüssel

Statusabelle T06 Fehlerhafte Angaben im Anfragesatz

Fehlercodes der DSRV

Text- bau- stein	Meldungen
D01	Schema Anfrage fehlerhaft
D02	Datenteil (Body) konnte nicht gefunden werden
D04	DSRV Connector konnte nicht aufgerufen werden
D05	CICS IBM Host Transaktion xxxx konnte nicht gefunden werden
D08	Technischer Fehler DSRV Connector
D09	Fehler beim Aufbau Response
D10	Timeout bei der Anfrage über den DSRV Connector
E10	Fehler, DSRV-Übernahme war noch erfolgreich

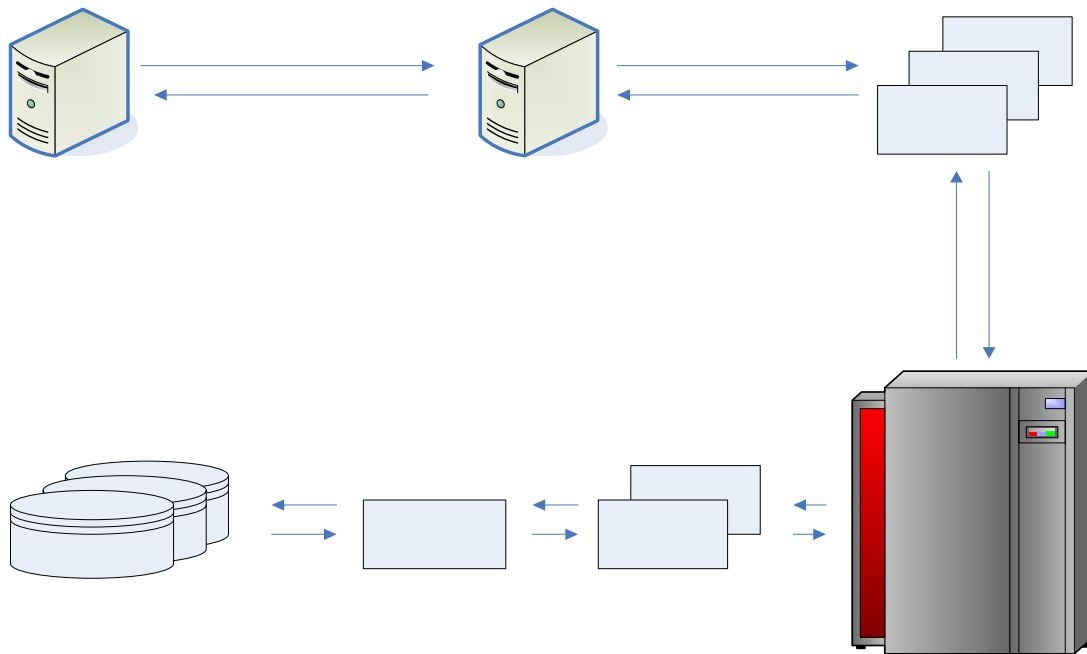
E11	Fehler, DSRV-Verarbeitung war noch erfolgreich
E96	Falscher Zeichensatz im Transport-Header (nicht ISO 8859-1)
T01	Lesefehler im SMSZ-Bestand
T02	Lesefehler im Perso-Bestand
T04	Lesefehler im Alpha-Suchbestand
T05	DSRV Doppelvergabeverdachtsprüfung, fehlerhafter Anfrageschlüssel
000	Daten wurden erfolgreich verarbeitet

### Doppelvergabeverdachtsprüfung bei der DSRV

Für Doppelvergabeverdachtsfälle hat der Organisationsausschuss der Rentenversicherung in seiner Sitzung 5/75 am 4. November 1975 (TOP 6) die Schnittstelle „Doppelvergabeverdacht“ auf 39 % und darunter festgelegt.

Die unter der Versicherungsnummer gelieferten persönlichen Daten werden gegen den Stammsatzbestand der DSRV (Datenstelle der Träger der Rentenversicherung) geprüft.

Liegt eine Übereinstimmung kleiner 40% vor, werden die Meldungen bei der DSRV mit „Doppelvergabeverdachtsfehler“ abgewiesen.



**Abbildung 9: DSVV Verarbeitung**

#### **3.4.1.2 Kommunikationsprotokoll**

Als Kommunikationsprotokoll wird ein intern abgestimmtes XML-basiertes Verfahren verwendet, das auf dem eXTra-Standard<sup>4</sup> aufbaut. Dies hat nicht zur Folge, dass diese

<sup>4</sup> Informationen zum eXTra-Standard sind unter [www.extra-standard.de](http://www.extra-standard.de) zu finden

Schnittstelle bei Änderungen des eXTra-Standards aktualisiert wird. Änderungen an der Schnittstelle werden ausschließlich über einen definierten Prozess unter Zustimmung aller Beteiligten bei entsprechendem Bedarf durchgeführt. Die Strukturen können den im Anhang XXX befindlichen Schnittstellenspezifikationen inklusive der Beispieldateien entnommen werden.

Im Echtbetrieb wird aus Performancegründen keine Schemavalidierung der Anfragen und Rückantworten durchgeführt. Der Nutzdatenteil kann sich innerhalb der „CharSequence“ bis zu 2000 mal wiederholen. Die einzelnen Nutzdatensätze sind durch ein „CRLF“ getrennt. Die CharWequence selbst darf sich nicht wiederholen.

Die Kommunikation erfolgt ausschließlich synchron über http. Die ZSS sendet ihre SendungsID in der RFV-Anfrage im Feld „RequestID“. Bei der Anfrage der RFV an DSRV wird die RequestID der ZSS weiter verwendet und durch die interne RequestID der RFV ergänzt. Die DSRV liefert in der ResponseID an die RFV ihre Ticket-Nummer. Die RFV ergänzt bei der Rückantwort an die ZSS ihre eigene ResponseID.

Dies wird durch folgendes Beispiel veranschaulicht:

Prozess	RequestID	ResponseID
ZSS-RFV Anfrage	12345	n.v.
RFV-DSRV Anfrage	12345_abcd	n.v.
RFV-DSRV Antwort	12345_abcd	98765
ZSS-RFV Antwort	12345	98765_zyxwv

### **3.4.2 Anfrage zur Vergabe einer vID/ZID zu einer Versicherungsnummer/Verfahrensnummer**

Die Meldesätze der Arbeitgeber müssen entweder mit einer vID oder einer ZID in der ZSS abgespeichert werden. Die hierzu notwendige Verknüpfung der VSNR bzw. Verfahrensnummer mit der ZID bzw. vID wird in der RFV abgespeichert. Der grundsätzliche Prozess, die technische Anbindung und die Kommunikationswege sind bereits in Abschnitt 3.3.1 beschrieben.

### RFV Kommunikationszustände

Fehlerklasse	Bemerkung
Keine Netzwerkverbindung	Die ZSS kann an die RFV nicht zugreifen (z. B. ein Netzwerkproblem).
Keine Serververbindung	Die ZSS kann an die RFV zugreifen, die http-Server melden jedoch einen Fehler (z. B. viel zu viele offene Verbindungen).
Halt	Kritische Probleme in der RFV-Infrastruktur, die ZSS soll bis auf weiteres keine Abfragen schicken.
Retry notwendig	Temporäre Probleme in der RFV-Infrastruktur, die ZSS soll die Abfragen nach einer kurzen Wartezeit wiederholen.
DSRV-Fehler	DSRV-Fehler lt. dem DSRV-Fehlerkatalog oder keine Antwort von DSRV.

### ZSS-Kommunikationszustände

Da die ZSS ausschließlich als Anfrage fungiert, ist hier keine nähere Beschreibung notwendig.

#### 3.4.2.1 Vergabe einer VID

Die Erzeugung einer VID wird von der RFV über einen automatisierten Prozess durchgeführt. Die so erzeugte VID wird bis zur Anmeldung des Teilnehmers als Ordnungskriterium in der ZSS verwendet.

Im Detail stellt sich der Prozess wie folgt dar:

Der AG überträgt den MVDS an die Zentrale Speicherstelle.

Die ZSS fragt über eine dedizierte VPN-Verbindung für einen empfangenen Meldesatz die RFV mit der VSNR bzw. mit der Verfahrensnummer und einer für die Plausibilitätsprüfung notwendige Attributmenge aus persönlichen Daten an und möchte für diese VSNR bzw. Verfahrensnummer, die zugehörige ZID ermittelt haben.

Solange sich der zu dieser VSNR gehörende Teilnehmer noch nicht zum Verfahren angemeldet hat und bislang noch keine Meldung zu diesem Teilnehmer abgegeben wurde, ist in der Datenbank der RFV keine Verknüpfung zwischen VSNR bzw. Verfahrensnummer und einer vID oder ZID vorhanden. In einem solchen Fall wird eine vID von der RFV vergeben. Diese ist analog zur Zertifikatsidentitätsnummer aufgebaut und muss eindeutig als vID erkennbar sein. Die RFV sorgt für die Eindeutigkeit dieser Nummer und für die Zuordnung der Nummer zur VSNR. Diese vID wird in der RFV-Datenbank als aktuell gültige ZID abgelegt und im Folgenden wie eine vollwertige ZID behandelt. Der Datensatz in der ZSS kann nun unter der vID gespeichert werden.

### **3.4.3 Bekanntgabe einer vergebenen Verfahrensnummer an den Teilnehmer**

Der Beamte, Richter oder Soldat wird gemäß § 97 Absatz 4 Satz 4 SGB IV über die Vergabe der Verfahrensnummer durch die DSRV schriftlich unterrichtet.



## 4 Löschung der Daten

### 4.1 ZSS

### 4.2 RFV

## 5 Anlagen

- Anlage 1 ELENA-Verfahrensgesetz
- Anlage 2 ELENA-Datensatzverordnung (noch nicht erschienen)
- Anlage 3 Gemeinsame Grundsätze
- Anlage 3a Gemeinsamen Grundsätze für die Erstattung der Meldungen der Arbeitgeber an die Zentrale Speicherstelle im Rahmen des Verfahrens des elektronischen Entgeltnachweises nach § 28b Absatz 6 SGB IV
- Anlage 3b Gemeinsamen Grundsätze zur Kommunikation zwischen der Zentralen Speicherstelle, der Registratur Fachverfahren und der Datenstelle der Träger der Rentenversicherung nach § 28b Absatz 6 SGB IV
- Anlage 3c Gemeinsame Grundsätze zur Kommunikation zwischen den ZSS und den abrufenden Stellen
- Anlage 4 Eckpunktekatalog des BMWi
- Anlage 5 Plausibilitäts- bzw. Kernprüfung des MVDS
- Anlage 5a Hinweise, die die ZSS an den Arbeitgeber sendet
- Anlage 5b Weitere Fehlermeldungen der Zentralen Speicherstelle im ELENA-Verfahren
- Anlage 6 Multifunktionaler Verdienstdatensatz Fachlicher Inhalt
- Anlage 7 Beschreibung von Sachverhalten bei Entgeltabrechnungen in Musterbeispielen

## **6 Anhänge**

### **6.1 Begriffsdefinitionen**

### **6.2 Tabellenverzeichnis**

### **6.3 Abbildungsverzeichnis**

Abbildung 1: Gesamtüberblick ELENA-Verfahren	9
Abbildung 2: Sicherheitszonen ZSS	13
Abbildung 3: Horizontale Trennung	16
Abbildung 4: Vertikale Trennung	17
Abbildung 5: Verarbeitung eines MVDS	44
Abbildung 6: Verarbeitung eines DSVV	45
Abbildung 8: Verarbeitungsprozess ZSS - DSRV	47
Abbildung 9 Übersicht über den Prozess	50
Abbildung 10: DSVV Verarbeitung	53