Diese Vorschrift ist nur
für den internen Gebrauch
bei der Polizei bestimmt.

PDV 870 **Ausgabe 2016**

Kryptobetriebsdienst

vereinnahmt	Datum	Beleg-Nr./ lfd. Nr.

Einführungserlass

Baden- Württemberg

Bayern

Berlin

Brandenburg

Bremen

Hamburg

Hessen

Mecklenburg-Vorpommern

Niedersachsen

Nordrhein-Westfalen

Rheinland-Pfalz

Saarland

Sachsen

Sachsen-Anhalt

Schleswig-Holstein

Thüringen

Bund

Einstufung gemäß Verschlusssachenanweisung
und
Regelungen für die Weitergabe

Es liegen keine Gründe für eine Einstufung gemäß Verschlusssachenanweisung oder Versagung der Weitergabe vor.

Änderungsnachweis

Änderung		Geändert		Unterschrift
Nr.	Datum	von Dienststelle	am	

Inhaltsverzeichnis

Anmerkung:
Soweit Personen- und Funktionsbezeichnungen aus Gründen der Lesbarkeit nur in der männlichen Form verwendet werden, gelten sie gleichermaßen für Frauen.

1 Allgemeines

1.1 Diese Vorschrift regelt den Kryptobetriebsdienst der Polizeibehörden und Polizeieinrichtungen, sofern der Kryptobetrieb mit Kryptosystemen durchgeführt wird, die für die Übertragung von Verschlusssachen (VS) vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen sind.

Sie ergänzt die

- Verschlusssachenanweisungen (VSA) der Länder und des Bundes und die diese ergänzenden Richtlinien

- PDV 810.1

1.2 Der Kryptobetriebsdienst hat die Aufgabe, VS-Nachrichten so zu übermitteln, dass deren Inhalte bei der Übertragung vor dem Zugriff und der Kenntnisnahme durch Unbefugte geschützt werden. Für die VS-Einstufung der Nachricht ist die herausgebende Stelle verantwortlich. Der Kryptobetrieb wird in Kryptobetriebsstellen durchgeführt.

Weitere Aufgaben des Kryptobetriebsdienstes sind

- Überwachen und Erhalten sowie ggf. Wiederherstellen der Kryptosicherheit

- Überwachen der Einhaltung der Vorschriften und Regelungen für den Kryptobetrieb

1.3 Bei dem Kryptobetrieb sind die IT-Sicherheitsfunktionen der eingesetzten IT-Produkte zu beachten und entsprechend anzuwenden.

1.3.1 Zutritt zu Kryptobetriebsstellen darf nur berechtigten Personen im Rahmen der jeweiligen Aufgaben gewährt werden.
Berechtigte Personen, die nicht zum Kryptobetriebsdienst gehören, sind während ihres Aufenthalts zu beaufsichtigen.

1.3.2 Unbesetzte Kryptobetriebsstellen sind zu verschließen. Bei Abwesenheit des Kryptobetriebspersonals von länger als einer Stunde sind zusätzlich die vorhandenen Sicherungseinrichtungen in Betrieb zu nehmen.

1.3.3 Elektronische Geräte, die nicht zwingend in der Kryptobetriebsstelle erforderlich sind, dürfen nicht eingebracht werden, z.B. Fernseh-, Hörfunk-, Ton-, Bildaufzeichnungs- und Wiedergabegeräte, Mobilfunktelefone.

1.3.4 Kryptomaterial und -unterlagen dürfen nur dem Kryptobetriebspersonal oder entsprechend Befugten im Rahmen der jeweiligen Aufgaben zugänglich gemacht werden. Ein Nachweis über die Verwendung und den Verbleib des Materials ist zu führen.

2 Kryptobetrieb

2.1 Grundsätze

2.1.1 Der Kryptobetrieb wird von Kryptobetriebspersonal, das entsprechend des jeweiligen Sicherheitsüberprüfungsgesetzes überprüft und ermächtigt wurde, in Kryptobetriebsstellen durchgeführt.

2.1.2 Es sind nur zugelassene Kryptosysteme einzusetzen, die vor ihrer Inbetriebnahme einer technischen Prüfung durch das BSI unterzogen wurden.

Als VS-Kommunikationssystem (Anlage 4) sind

- Kryptogeräte

- VS-Endgeräte und

- Peripheriekomponenten

einzusetzen, die aufgrund einer vom BSI durchgeführten Abstrahlmessung für den Einsatz in den vorgesehenen Kryptobetriebsstellen geeignet und zugelassen bzw. freigegeben sind.

2.1.3 Die möglichen Übertragungsverfahren sowie die spezifische Handhabung der eingesetzten Kryptogeräte, VS-Endgeräte und Peripheriekomponenten werden in den Anlagen 1, 2 und 3 erläutert.

2.2 Schutz des VS-Kommunikationssystems

2.2.1 Das VS-Endgerät und die Peripheriekomponenten sind so zu konfigurieren, dass nur die für das Erstellen, das Versenden, den Empfang, die Löschung und die Dokumentation dieser Tätigkeiten ausschließlich erforderliche Software genutzt werden kann bzw. nur freigegebene Funktionen genutzt werden können. Wiederholt abgewiesene Zugriffsversuche sollen für den betreffenden Nutzer zu einer System-/Anmeldesperre führen.
Andere als die zugelassenen und über Kryptiertechnik gesicherten Netzanbindungen sind zu verhindern.

2.2.2 Auf dem VS-Endgerät ist ein Virenschutzprogramm zu installieren, mit dem alle eingehenden und ausgehenden Nachrichten überprüft werden.

2.2.3 Das Virenschutzprogramm und die Virensignaturen sind auf dem neuesten Stand zu halten. Bei Virenbefall ist der Verantwortliche für IT-Geheimschutzmaßnahmen unmittelbar zu informieren, um geeignete Maßnahmen abzusprechen und zu ergreifen.
Infizierte Dateien dürfen weder geöffnet noch übermittelt werden.

2.2.4 Die Konfiguration der Hard- und Software ist zu dokumentieren; die Unterlagen und eine Referenzkopie der Software sind gegen unberechtigte Veränderungen zu schützen und so aufzubewahren, dass sie im Bedarfsfall nutzbar sind.

2.3 Behandlung von VS-Datenträgern/ausgedruckten VS

2.3.1 Die Ausgabe von VS-Datenträgern und ausgedruckten VS, ihr Verbleib und ihre Vernichtung werden vom Kryptobetriebspersonal entsprechend den gültigen Vorschriften nachgewiesen.

2.3.2 VS-Datenträger mit nicht kryptierten Verschlusssachen sind mit dem höchsten Geheimhaltungsgrad der darauf gespeicherten VS gemäß der VSA zu kennzeichnen und entsprechend den gültigen Vorschriften nachzuweisen.

2.3.3 Die Weitergabe/Beförderung von VS-Datenträgern oder ausgedruckten VS richtet sich nach den Bestimmungen der VSA oder den ergänzenden Richtlinien zur VSA.

2.3.4 Die Freigabe bzw. Wiederaufbereitung von VS-Datenträgern für eine Nutzung in anderen Einsatzbereichen ohne entsprechende VS-Zugriffsberechtigung ist auch nach ihrer Löschung nicht zulässig.

2.3.5 Defekte, nicht verwendbare VS-Datenträger sind über die VS-Registratur physikalisch zu vernichten.

3 Durchführung des Kryptobetriebes

3.1 Grundsätze

Abhängig von den Empfangsmöglichkeiten des Empfängers können VS als Fax oder als Datei übermittelt werden. Falls eine sofortige Bearbeitung von VS notwendig ist, ist vor Übermittlung der Empfänger telefonisch zu informieren.

3.2 Aufbereitung der VS zur Übermittlung

In Abhängigkeit von der Erstellungsform werden

- VS in Papierform eingescannt
- auf einem VS-Datenträger angelieferte VS auf Viren überprüft und in das VS-Endgerät eingelesen
- auf dem VS-Endgerät erstellte VS in einem entsprechenden Verzeichnis abgespeichert

Die VS stehen dann in elektronischer Form im VS-Endgerät für den Versand als Fax oder als Datei bereit.

3.3 Übermittlung

3.3.1 Vor der Übermittlung muss jede VS im VS-Bestandsverzeichnis der VS-Registratur erfasst und mit einer VS-Tagebuchnummer, einschließlich der Abkürzung des Geheimhaltungsgrades, versehen sein. Ist dies infolge besonderer Dringlichkeit oder aus anderen zwingenden Gründen zunächst nicht möglich, so ist die VS-Registratur davon unverzüglich zu unterrichten.

3.3.2 Regelungen zur Übermittlung der VS sind in den Anlagen 1 und 2 enthalten.

3.3.3 Jeder Empfang einer VS ist unmittelbar der absendenden Kryptobetriebsstelle zu bestätigen.

3.4 Protokollierung

Das VS-Endgerät ist so zu konfigurieren, dass ein Übertragungsprotokoll erstellt wird.
Auf Anforderung ist dem Aufgeber der VS das entsprechende Übertragungsprotokoll auszuhändigen.

Die Protokolle sind aufzubewahren und zu Prüfzwecken den Geheimschutzbeauftragten und den Verantwortlichen für IT-Geheimschutzmaßnahmen zugänglich zu machen.
Die Aufbewahrungsfrist beträgt mindestens 10 Jahre.

3.5 Löschung

Nach erfolgreichem Versand der VS ist die auf dem VS-Endgerät gespeicherte VS – sofern diese nicht mehr zur Weiterverarbeitung benötigt wird – mit der hierfür bereitgestellten Löschsoftware/-funktion zu löschen. Gleiches gilt für empfangene VS.

4 Sicherheitsvorkommnisse

Wird bekannt oder besteht der Verdacht, dass

- Bestimmungen der VSA oder der diese ergänzenden Richtlinien oder dieser Vorschrift verletzt worden sind

- Unbefugte von einer Verschlusssache Kenntnis erhalten haben

- eine Verschlusssache, Kryptomaterial, ein Schlüssel zu einem VS-Verwahrgelass, zu Schließfächern eines VS-Schlüsselbehälters, zu einer Kryptobetriebsstelle oder zum Ein- und Ausschalten einer Gefahrenmeldeanlage abhanden gekommen ist oder

- das Kryptosystem bzw. Kryptomaterial oder sonstige IT-Komponenten manipuliert worden sind

so sind unverzüglich der Verantwortliche für IT-Geheimschutzmaßnahmen und der Geheimschutzbeauftragte zu benachrichtigen.

Sie sind auch zu benachrichtigen bei Beobachtungen und Ereignissen, die unter dem Gesichtspunkt der Informations- und Kommunikationssicherheit von Bedeutung sind.

5 Betriebsbereitschaft

Zur Sicherung der Betriebsbereitschaft des Systems sind monatlich Betriebsmitteilungen mit mindestens einer Gegenstelle auszutauschen.

6 Notfallkonzeption

6.1 Die Betriebsbereitschaft des Kryptosystems ist sicherzustellen.

6.2 Zur Aufrechterhaltung des Kryptobetriebes im Störungsfall ist für die Kryptobetriebsstellen eine Notfallkonzeption zu erstellen. Dies muss mindestens Aussagen über geeignete Umleitwege, Vorhalt von Ersatzsystemen, sachliche Zuständigkeiten und Reaktionszeiten im Störungsfall enthalten.

Datei-Übertragung

1 Ausgang

1.1 Die entsprechend aufbereitete VS wird mit dem Dateiübertragungsprogramm übermittelt. Hierzu werden der Servermodus des Dateiübertragungsprogramms abgeschaltet, der Empfänger aus dem Adressbuch ausgewählt und die Dateiübermittlung gestartet.

1.2 Empfänger, die noch nicht im Adressbuch eingetragen sind, sind nachzutragen.

1.3 Nach der VS-Übermittlung ist der Servermodus sofort wieder zu aktivieren, um damit die Empfangsbereitschaft herzustellen.

1.4 Erfolgreich übermittelte VS sind grundsätzlich nach Ausdruck der Übertragungsbestätigung zu löschen (Nr. 3.5).

2 Eingang

2.1 Standardmäßig befindet sich das Dateiübertragungsprogramm in Empfangsbereitschaft (Servermodus). Sollte dies nicht der Fall sein, ist zur Herstellung der Empfangsbereitschaft das Dateiübertragungsprogramm zu starten und der Servermodus zu aktivieren.

2.2 Als Dateien eingehende, empfangene VS sind auf Viren zu prüfen und im entsprechenden Eingangsordner auf der Festplatte des VS-Endgerätes abzulegen. Anschließend sind die Dateien auf VS-Datenträger des Empfängers zu kopieren oder unmittelbar auszudrucken.

Werden VS ausgedruckt, ist auf dem Ausdruck der Geheimhaltungsgrad gemäß VSA anzubringen.

2.3 Nach erfolgreichem Kopieren der VS auf VS-Datenträger oder Ausdrucken einer empfangenen VS ist die auf dem VS-Endgerät gespeicherte VS, sofern sie nicht mehr zur Weiterverarbeitung benötigt wird, zu löschen (Nr. 3.5).

noch Anlage 1

Telefax-Übertragung

1 Ausgang

1.1 Die entsprechend aufbereitete VS wird mit Hilfe des Faxprogramms/ Faxgerätes unter Auswahl des Empfängers aus dem Adressbuch übermittelt.

1.2 Empfänger, die noch nicht im Adressbuch eingetragen sind, sind nachzutragen.

1.3 Erfolgreich übermittelte VS sind grundsätzlich nach Ausdruck der Übertragungsbestätigung zu löschen oder dem Aufgeber zurückzugeben (Nr. 3.5).

2 Eingang

2.1 Standardmäßig befindet sich die Fax-Software/das Faxgerät in Empfangsbereitschaft. Sollte dies nicht der Fall sein, ist zur Herstellung der Empfangsbereitschaft das Fax-Programm zu starten bzw. das Faxgerät einzuschalten.

2.2 Die Fax-Software/das Faxgerät ist so einzustellen, dass eingehende Faxnachrichten sofort ausgedruckt werden.

2.3 Nach erfolgreichem Kopieren der VS auf VS-Datenträger oder Ausdrucken einer empfangenen VS ist die auf dem VS-Endgerät gespeicherte VS, sofern sie nicht mehr zur Weiterverarbeitung benötigt wird, zu löschen (Nr. 3.5).

noch Anlage 2

Anlage 3

Fernmündliche Kommunikation

Zur fernmündlichen Kommunikation kann an den ISDN-Verteiler zusätzlich ein ISDN-Telefon entsprechend der Anlage 4 oder über einen Terminaladapter ein analoges Telefon angeschlossen werden.

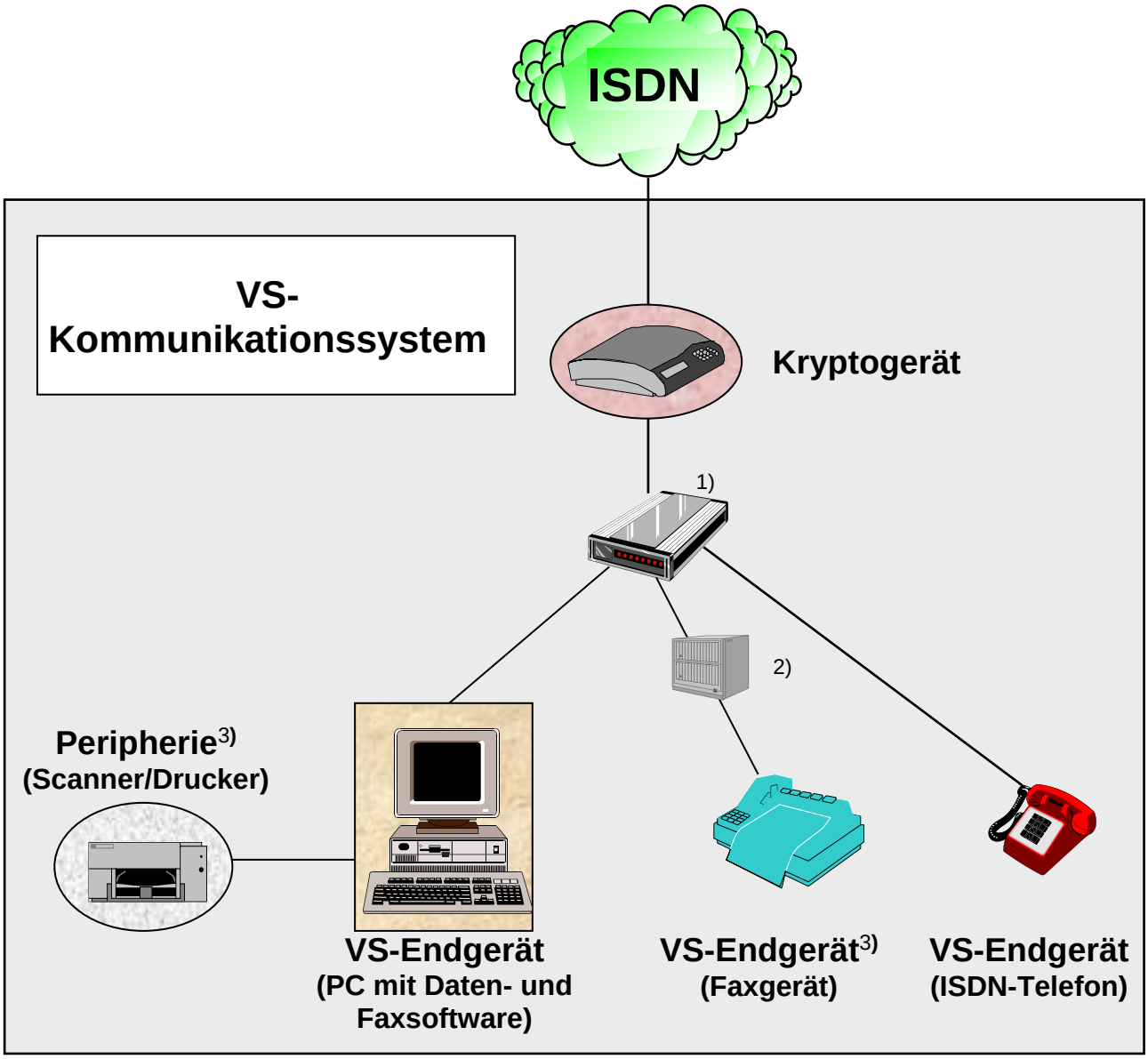
Vorrangig ist das Telefon zur VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften mündlichen Kommunikation zwischen Empfänger und Kryptobetriebsstelle zwecks Absprache von Übertragungen/Tests zu verwenden.

Bei Verwendung des Telefons für Gespräche zu VS-VERTRAULICH oder höher eingestuften VS sind die VSA oder die diese ergänzenden Richtlinien zu beachten.

noch Anlage 3

Anlage 4

VS-Kommunikationssystem
(Schematische Darstellung)



1) ISDN-Verteiler
2) Terminaladapter (Digital-/Analog-Wandler)
3) Alternativ kann als Peripherie oder VS-Endgerät (Faxgerät) auch ein Multifunktionsgerät eingesetzt werden.

noch Anlage 4