

Dienstanweisung über die Einführung der elektronischen Signatur und chipkartenbasierten Verschlüsselung

§ 1

Geltungsbereich

Diese Dienstanweisung ergänzt die bestehende Dienstanweisung über die Einführung E-Mail, Intranet und Internet für den Zeitraum des Projektes SiNiKOM.

§ 2

Zweckbestimmung

- (1) Die Elektronische Signatur und die chipkartenbasierte Verschlüsselung dienen der gesicherten Kommunikation der Beschäftigten mit externen Stellen sowie untereinander. Sie ermöglichen, nunmehr auch Daten der Schutzstufen C und D (Anlage 1) per elektronischer Post zu übermitteln.
- (2) Die Nutzung erfolgt nur zu dienstlichen Zwecken.
- (3) Die Karte ist mit dem Aufgabenwechsel/Ausscheiden aus dem Dienst grundsätzlich an das Hauptamt, EDV-Bereich, zurückzugeben.

§ 3

Vertretungsregelung

- (1) Bei vorhersehbarer Abwesenheit ist eine automatische Antwort an den Absender zu schicken mit dem Hinweis auf die Dauer der Abwesenheit und die Vertretung, an die die Post weitergeleitet wird. Die Vertretung setzt sich mit dem Absender in Verbindung und teilt diesem das zu nutzende Zertifikat mit.
- (2) Um bei Abwesenheit den Zugriff auf bereits früher eingegangene E-Mails sicherzustellen, dürfen E-Mails und Dokumente nur für den Transport verschlüsselt werden. Die Speicherung hat grundsätzlich unverschlüsselt zu erfolgen.

§ 4

Umgang mit verschlüsselten E-Mails an Gruppen

- (1) Neben den personenbezogenen E-Mail Adressen werden auch sog. Bereichsadressen genutzt. Hierzu können anonymisierte und geschlossene Benutzergruppen (z. B. Sozialämter im Landkreis) gehören.

- (2) Den Organisationseinheiten (Ämtern, Organisationsadressen) wird eine Bereichskarte zugeordnet. Diese Karte kann nicht zur Signatur eingesetzt werden. Die Organisationseinheit ist für die ordnungsgemäße zentrale Aufbewahrung der Bereichskarte und der zugehörigen PIN verantwortlich.

§ 5

Einsatz und Nutzung der Message-Recovery Card

- (1) Die Message-Recovery Card hat die Aufgabe, E-Mails und Dokumente zu entschlüsseln, die nach den bisherigen Regelungen nicht zu bearbeiten wären. Daraus ergibt sich das Einsatzgebiet ausschließlich in folgenden Fällen:
- Verlust bzw. Unbrauchbarkeit der Karte
 - Längerfristige Abwesenheit des Kartenbesitzers / der Kartenbesitzerin
 - Ausscheiden des Kartenbesitzers / der Kartenbesitzerin aus dem Dienst.
- (2) Nachrichten sind grundsätzlich für die Message-Recovery-Card mit zu verschlüsseln.
- (3) Die Message-Recovery Card und die PIN sind gesichert aufzubewahren. Die Herausgabe der Karte erfolgt auf schriftlichen, zu begründenden Antrag und ist von der zuständigen Amtsleitung gegenzuzeichnen; die Rückgabe ist zu dokumentieren.

§ 6

Umgang mit fehlerhaft zertifizierten E-Mail

- (1) Erhalten Bedienstete eine E-Mail mit einem ungültigen oder unbrauchbaren Zertifikat, so ist die betroffene Nachricht an die Administration zur weiteren Veranlassung weiterzuleiten.
- (2) Erhalten Bedienstete eine E-Mail mit einer nicht lesbaren Verschlüsselung, ist diese mit einem entsprechenden Hinweis an den Absender / die Absenderin zurückzusenden und erneut anzufordern.

§ 7

Umgang mit Viren in verschlüsselten Nachrichten

- (1) Vor der Installation der zur Teilnahme am Verfahren notwendigen Komponenten ist sicherzustellen, dass auf dem Arbeitsplatz eine Virenschutzsoftware installiert wurde. Die Virensignaturen werden laufend systemseitig aktualisiert. Eine zentrale Lösung auf einem Mail-Server genügt nicht den Anforderungen.

- (2) Sind verschlüsselte und/oder signierte Nachrichten eingegangen, die einen Virus enthalten, ist die Nachricht ungeöffnet zu löschen und der Absender / die Absenderin zu informieren.

§ 8

Inkrafttreten

Diese Dienstanweisung tritt mit ihrer Unterzeichnung in Kraft.

Stadthagen, den 16.01.2003

Heinz-Gerhard Schöttelndreier
Landrat

Anlage 1**Schutzstufen**

Die Datenschutzmaßnahmen müssen angemessen sein. Ob eine Maßnahme als ausreichend anzusehen ist, kann grundsätzlich nur im Einzelfall entschieden werden. Als Orientierungshilfe und Maßstab für ein abgestuftes Sicherungskonzept sind folgende Schutzstufen anzusehen:

- Stufe A: Frei zugängliche Daten, in die Einsicht gewährt bzw. über die Auskunft erteilt wird, ohne dass der Einsichtnehmende ein berechtigtes Interesse geltend machen muss, z.B. Adress- und Telefonbücher, Namenslisten vom Kreistag und seinen Ausschüssen, einfache Melderegisterauskunft.
- Stufe B: Personenbezogene Daten, deren Missbrauch zwar keine besondere Beeinträchtigung erwarten lässt, deren Kenntnisnahme jedoch an ein berechtigtes Interesse des Einsichtnehmenden gebunden ist, z.B. einfache Gewerbe- registerauskunft, Katasterauskunft.
- Stufe C: Personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann ("Ansehen"), z.B. Angaben zum Einkommen, Ordnungswidrigkeiten, Sozialdaten soweit nicht Stufe D.
- Stufe D: Personenbezogene Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann ("Existenz"), z.B. medizinische oder psychologische Untersuchungsergebnisse, Beurteilungen, Schulden, Straffälligkeit.
- Stufe E: Personenbezogene Daten, deren Missbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann, z.B. Daten über Personen, die selbstmordgefährdet sind oder die aufgrund der Informationen Opfer einer Straftat werden können.