

Das Beispiel ELENA: Sichere Verschlüsselung ist möglich! Aber ist sie auch politisch gewollt?

Werner Hülsmann
Diplominformatiker, Datenschutzsachverständiger und Mitglied
• der Deutschen Vereinigung für Datenschutz (DVD) e.V. und
• des Beirats des Forum InformatikerInnen für Frieden und
gesellschaftliche Verantwortung (FIff) e.V.

© 2010 - Werner Hülsmann - www.Datenschutzwissen.de

Zu meiner Person

1982 – 1988 Studium der Informatik an der TU Darmstadt
Schwerpunkt Datenschutzrecht
1988 – 1991 Softwareentwickler bei der Telenorma GmbH, Frankfurt (Main)
1992 – 1999 Wissenschaftlicher Mitarbeiter und Referatsleiter Technik beim Landes-
beauftragten für den Datenschutz der Freien Hansestadt Bremen
1999 – 2001 Datenschutz- und Technologieberatung bei ForBIT e.V. in Hamburg
Seit 1999 selbständiger Datenschutzberater (Datenschutzconsulting.eu)
2001-2003 Projektmanager Dataprotection bei der Telegate AG (Martinsried)
2003 - 2009 Mitglied im Vorstand der Deutschen Vereinigung für
Datenschutz (DVD) e.V., Bonn - www.datenschutzverein.de
Seit 2004 Kooperationspartner des virtuellen Datenschutzbüros
2004 Gründung von Datenschutzwissen.de – Organisation und Leitung von
Datenschutzseminaren
Seit 2004 beim Unabhängigen Landeszentrum für Datenschutz Schleswig-
Holstein anerkannter Sachverständiger für IT-Produkte
(rechtlich/technisch)
Seit 2010 Mitglied des Beirat des Forums InformatikerInnen für Frieden und
gesellschaftliche Verantwortung (FIff) e.V.
Seit 2010 Expert for legal and technical evaluations for the European
Privacy Seal (EuroPriSe, <http://www.european-privacy-seal.eu/>)



© 2010 - Werner Hülsmann - www.d-s-c.info

ELENA



- ... steht für **Elektronischer Entgeltnachweis**
- ... ersetzt ab 2012 die bisherigen jährlich 60 Millionen Lohn- und Gehaltsbescheinigungen, die für die unterschiedlichen Behörden bei der Beantragung von Sozialleistungen wie
 - Wohngeld
 - Elterngeld
 - Arbeitslosengeld (I und II)von den AntragstellerInnen benötigt und von den ArbeitgeberInnen ausgestellt werden.
- ... soll den ArbeitgeberInnen jährlich Kosten in Höhe von über 80 Millionen Euro einsparen

(vgl. <https://www.das-elena-verfahren.de/was-ist-elena>)

© 2010 - Werner Hülsmann - www.d-s-c.info

ELENA

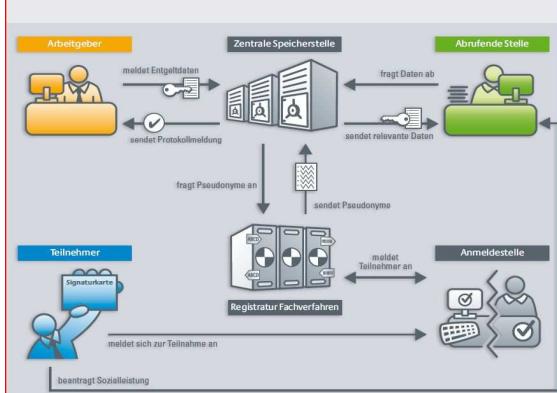


- ... erspart ab 2012 AntragstellerInnen den Gang zu ihrem/ihrer ArbeitgeberIn, der/die dann die Beantragung von Sozialleistungen nicht mehr mitbekommt.
- ... bedingt, dass ab 2012 jedeR AntragstellerIn eine digitale Signaturkarte benötigt.
- ... ist vom Bundestag am 29. März 2009 mit dem „Gesetz über das Verfahren des elektronischen Entgeltnachweises (ELENA Verfahrensgesetz)“ beschlossen worden
- ... hat bereits im Oktober 2008 den BigBrotherAward in der Kategorie Politik erhalten (vgl. <https://www.bigbrotherawards.de/2008/.pol/>)

© 2010 - Werner Hülsmann - www.d-s-c.info

Wie funktioniert ELENA?

Das ELENA-Verfahren – so funktioniert's:



Quelle: <http://www.piratenbrandenburg.de/tag/piratenpartei/> Eintrag vom 31.12.2009

© 2010 - Werner Hülsmann - www.d-s-c.info

ELENA

- Nahezu jede/r ArbeitgeberIn ist verpflichtet monatlich die Daten der ArbeitnehmerInnen an die Zentralstelle zu melden
 - Ausnahme: Haushaltsnahe geringfügig Beschäftigte nach § 8a des Vierten Buches Sozialgesetzbuch (SGB IV)
- Dabei ist ein sehr umfangreicher Datensatz zu übermitteln
 - Name, Anschrift, Steuerklasse
 - Arbeitszeit, Entgelt
 - Fehlzeiten
 - Bei Kündigung auch Abmahnungen im Vorfeld der Kündigung und Kündigungsgründe
 - ...

© 2010 - Werner Hülsmann - www.d-s-c.info



ELENA – Datenfelder im Detail

- Fehlzeiten
 - 03: Mutterschutzfrist
 - 06: Pflegezeit
 - 11: sonstige unbezahlte Fehlzeit (z.B. unentschuldbiges Fehlen/Arbeitsbummeli/Wochenende oder Feiertage ohne Entgelt/Pflege eines kranken Kindes/kurzzeitige Arbeitsverhinderungen wegen Pflege)
 - 12: unrechtmäßiger Streik*)
 - 14: rechtmäßiger Streik*)
 - 15: Aussperrung*)

*) Nach Protesten inzwischen gestrichen

© 2010 - Werner Hülsmann - www.d-s-c.info



Technokratie?

- ELENA ist eine **technische** Lösung für ein **gesellschaftliches** und sich daraus ergebendes **organisatorisches** Problem
- Es ist nicht nachvollziehbar, wieso keine gesellschaftliche oder zumindest organisatorische Lösung gesucht wird!

© 2010 - Werner Hülsmann - www.d-s-c.info

Technokratie?



- Organistorisches Problem:
Es gibt sehr, sehr viele verschiedene Einkommensbescheinigungsformulare für die Beantragung unterschiedlicher Sozialleistungen
 - Lösung: Die SGB-Anforderungen werden so vereinheitlicht, dass eine (standardisierte) Lohn- bzw. Gehaltsabrechnung den Anforderungen genügt
 - Vorteile:
 - ArbeitgeberInnen sparen nicht nur Kosten für das Ausstellen der vielen verschiedenen Bescheinigungen, sondern auch noch die Kosten für das ELENA-Verfahren
 - ArbeitnehmerInnen müssen keine Einkommensbescheinigungen mehr beim Arbeitgeber anfordern (Datenschutz!)

© 2010 - Werner Hülsmann - www.d-s-c.info

Technokratie?



- Gesellschaftliches Problem:
Es gibt Menschen, die Sozialleistungen für ihren Lebensunterhalt benötigen
- Lösung:
Bedingungsloses Grundeinkommen
- Vorteile
 - Es sind keinerlei Gehalts- oder Einkommensbescheinigungen mehr erforderlich
 - In der Sozialverwaltung könnten immense Bürokratiekosten eingespart werden.

© 2010 - Werner Hülsmann - www.d-s-c.info

Noch Fragen?

- Vielen Dank für Eure/Ihre Aufmerksamkeit



© 2010 - Werner Hülsmann - www.d-s-c.info

Kritik an ELENA

ELektronischer ENtgeltNACHweis

© 2010 - Werner Hülsmann - www.d-s-c.info

ELENA – Kritikpunkte



- Nach der aktuellen Rechtslage ist für den Zugriff auf die ELENA-Daten die Freigabe (mit digitaler Signatur) des Antragstellers bzw. der Antragstellerin erforderlich
- Für den Zugriff auf die Daten müssen zwei Behörden zusammenarbeiten (die zentrale Speicherstelle und die Registratur Fachverfahren)
- Technisch ist die Freigabe der Betroffenen allerdings nicht erforderlich!
 - Die Daten sind zwar verschlüsselt, aber mit einem zentralen Schlüssel!
 - Wenn beide Behörden zusammenarbeiten, ist ein Zugriff auf die Daten auch ohne Mitwirkung der Betroffenen möglich



ELENA – Kritikpunkte

- Durch Gesetzesänderungen lässt sich der technisch mögliche Datenzugriff auch für andere Behörden leicht legalisieren!
- Die bisherigen Erfahrungen (u.a. mit Mautdaten, TK-Vorratsdaten) zeigen, dass derartige Datensammlungen bei Politik und Wirtschaft Begehrlichkeiten wecken
- Ein Schutz, der nur durch gesetzliche Regelungen erreicht wird, kann jederzeit abgeschwächt oder aufgehoben werden!
- Die einheitliche Verschlüsselung aller Datensätze mit einem Schlüssel birgt ein hohes Risiko!

ELENA – Kritikpunkte



- Ob die vorgerechneten Einsparungen bei den ArbeitgeberInnen tatsächlich eintreten ist fraglich
 - Für kleine und viele mittlere Betriebe bedeutet ELENA einen zusätzlichen Aufwand.
 - Bei Kleinstbetrieben mit einem/einer oder mehreren geringfügigen Beschäftigten führt ELENA zu einen erheblichen Mehraufwand
 - Bisher (bei gleich bleibendem Einkommen): einmal jährliche Meldung zur Sozialversicherung,
 - Jetzt: monatliche Meldung

© 2010 - Werner Hülsmann - www.d-s-c.info



ELENA – Kritikpunkte

- ELENA ist „**eine Vorratsdatenspeicherung von sensiblen Daten**, die bei dem größten Teil der Bevölkerung für die ursprünglichen Zwecke nicht benötigt wird“

(Thilo Weichert, Leiter des Unabhängigen Landeszentrum für Datenschutz in seiner Pressemitteilung vom 25. Juni 2008, <https://www.datenschutzzentrum.de/presse/20080625-elena.htm>)

© 2010 - Werner Hülsmann - www.d-s-c.info

ELENA – Kritikpunkte



- "Große Datensammlungen erzeugen immer große Begehrlichkeiten. Überlegen Sie, was ein ausländischer Geheimdienst mit diesen Daten anfangen könnte oder wie attraktiv die Einkommensdaten eines ganzen Landes für ein Gangstersyndikat sind. Und es ist natürlich einfacher, einmal eine Verschlüsselung zu knacken und dann den Zugriff auf einen großen Pool zu haben, als jeden Datensatz einzeln entschlüsseln zu müssen."
- (Thilo Weichert, Leiter des Unabhängigen Landeszentrum für Datenschutz im Interview mit der TAZ am 28.12.2009, <https://www.taz.de/1/politik/schwerpunkt-ueberwachung/artikel/1/zu-90-prozent-nicht-benoetigt/>)

© 2010 - Werner Hülsmann - www.d-s-c.info



ELENA – Kritikpunkte

- „Im ELENA-Verfahren besteht ab 2010 für den Teilnehmer ein Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten. Eine Auskunft ist vor 2012 aber nicht realisierbar, da der Abruf durch die abrufenden Stellen erst ab 2012 möglich ist.“
(Quelle: <https://www.das-elena-verfahren.de/fragen-und-antworten/selbstauskunft/selbstauskunft>)
- Da selbst die Arbeitgeber nicht nachprüfen können, ob die Daten korrekt übermittelt wurden ist das Risiko von strittigen oder versehentlich falschen Daten enorm!

© 2010 - Werner Hülsmann - www.d-s-c.info

Wie mit der Verwendung von Einmalschlüsseln ein Datenzugriff ohne Beteiligung der Betroffenen technisch verhindert werden kann

© 2010 - Werner Hülsmann – www.Datenschutzwissen.de



Einmalschlüssel – eine technische Alternative

- Technisch und praktisch wären Verfahren möglich, bei denen ein Zugriff auf die Entgeltdaten nur mit Beteiligung der Betroffenen möglich wäre.
 - Arbeitgeber erstellt elektronischen Entgeltnachweis
 - Dieser wird mit einem ausreichend langen und ausreichend zufälligen Einmalschlüssel verschlüsselt.
 - Einmalschlüssel wird mit öffentlichem Schlüssel des/der Beschäftigten verschlüsselt
 - Für jeden Entgeltnachweis wird jeweils ein neuer Einmalschlüssel erstellt. Über eine Referenznummer wird der Zusammenhang zwischen verschlüsseltem Entgeltnachweis und verschlüsselten Einmalschlüssel hergestellt.

© 2010 - Werner Hülsmann - www.d-s-c.info

Einmalschlüssel – eine technische Alternative



- Eine zentrale Speicherung der verschlüsselten Entgelt-nachweise sowie der verschlüsselten Einmalschlüssel bei zwei verschiedenen Stellen stellt **keine** Vorratsdaten-speicherung dar, da ein Zugriff auf einen Entgelt-nachweis **nur** möglich ist, wenn der/die Beschäftigte den jeweiligen Einmalschlüssel mit seinem/ihren privaten Schlüssel entschlüsselt!
 - Ohne den privaten Schlüssel der Betroffenen stellen die gespeicherten Daten nur „Pseudodaten“ da.
 - Verliert der Betroffene seinen geheimen Schlüssel, sind die dazugehörigen Pseudodaten sogar nur noch Datenmüll

Einmalschlüssel – eine technische Alternative



- Verfahren zur Erzeugung ausreichend langer und ausreichend zufälliger Einmalschlüssel existiert.
- Verfahren zur sicheren Verschlüsselung und Speicherung der Daten und Pseudodaten existiert
- Vgl. hierzu auch das mit dem ULD-Datenschutzgütesiegel versehene Produkt Pseudodatenpool:
<https://www.datenschutzzentrum.de/guetaesiegel/kurzgutachten/g080604/>

ELENA – Aktivitäten gegen ELENA



- Weitere Informationen:
<http://wiki.vorratsdatenspeicherung.de/ELENA>
oder <http://wiki.stoppt-elena.de>
- Verfassungsbeschwerde gegen ELENA:
<https://petition.foebud.org/ELENA>
- Flyer:
 - zum Selbstausdrucken:
<http://wiki.vorratsdatenspeicherung.de/images/Elena-15.pdf>
 - zum Bestellen:
https://shop.foebud.org/product_info.php?pName=flyer-elena-p-471



ELENA – Aktivitäten gegen ELENA

- Aktivitäten der Gewerkschaften
 - Von Fehlanzeige bis zur Unterstützung der Verfassungsbeschwerde durch ver.di
- Parlamentarische Initiativen
 - Bundestagsfraktion der Grünen hat beschlossen einen Antrag in den Bundestag einzubringen
 - Inhalt: Reduzierung des Datensatz auf eine Minimum.
 - Der Antrag geht leider nicht auf den grundsätzlichen Kritikpunkt der Verwendung eines Generalschlüssels ein.
- Aktivitäten von Dir/Ihnen
 - Elena-Flyer ausdrucken oder bestellen und verteilen
 - Mit den Bundestagsabgeordneten des Wahlkreises sprechen
 - ...

Aktiv werden für den Erhalt der Privatsphäre?

- Unterstützen Sie durch Spenden und/oder aktive Mitarbeit Datenschutz- und Bürgerrechtsorganisationen, beispielsweise:
 - Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (www.fiff.de)
 - Deutsche Vereinigung für Datenschutz e.V. (www.datenschutzverein.de)
 - FoBueD e.V. (www.foebud.org)
- Informieren und sensibilisieren Sie Ihre Umgebung für den Wert der Privatsphäre und des Datenschutzes

© 2010 - Werner Hülsmann - www.d-s-c.info

Linktipps

- <http://www.bfdi.de> (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit)
- <https://www.datenschutzzentrum.de> (Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein)
- <http://www.datenschutz.de> (virtuelles Datenschutzbüro des Bundes- und der Landesbeauftragten für den Datenschutz sowie der Datenschutzaufsichtsbehörden)
- <https://www.bigbrotherawards.de/> (Big Brother Awards, Negativpreise für Datenkraken)
- <http://www.datenschutzverein.de/> (Deutsche Vereinigung für Datenschutz e.V., Bonn)
- <http://www.fiff.de> (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., Bremen)

© 2010 - Werner Hülsmann - www.d-s-c.info



Kontaktdaten

- Werner Hülsmann
E-Mail: werner@fiff.de
Obere Laube 48 – 78462 Konstanz
Tel.: 07531 / 365 90 56 – mobil: 0179 / 46 86 484
- Deutsche Vereinigung für Datenschutz (DVD) e.V.
Bonner Talweg 33-35 - 53113 Bonn
E-Mail: dvd@datenschutzverein.de
Internet: www.datenschutzverein.de
- Forum InformatikerInnen für Frieden und
gesellschaftliche Verantwortung (FIff) e.V.
Goetheplatz 4 – 28203 Bremen
E-Mail: fiff@fiff.de
Internet: www.fiff.de