



**TeleTrust**

*Pioneers in IT security.*

1989 25 Jahre 2014

## TeleTrust-interner Workshop

Berlin, 05.06.2014

# Common-eID – Interoperabilität für elektronische Ausweise

Dr. Detlef Hühnlein  
ecsec GmbH

## Presseinformation



# „Common-eID“ für leichtere Nutzbarkeit der Online-Ausweisfunktion

[Berlin, 29. April 2014] Führende Technologieanbieter im Umfeld elektronischer Identitäten (eID) haben ihre Kräfte im „Common-eID“ Projekt (<http://Common-eID.org>) gebündelt, um die Interoperabilität in diesem Bereich zu verbessern und dadurch diese wichtige Schlüsseltechnologie noch leichter nutzbar zu machen. Auf Basis der Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sollen systematische Tests mit den Client- und Server-Komponenten der unterschiedlichen Anbieter für das reibungslose Zusammenspiel sorgen.

## Motivation für Common-eID

- nPA-Zwischenbilanz nach 3,5 Jahren **eher ernüchternd**
  - existierende eID-Clients, eID-Server, eID-Services etc.
  - Anzahl an Diensteanbietern kaum steigend
  - kaum tatsächlich nutzbare Anwendungsdienste
- ... trotz des **sehr klaren** Bedarfs für starke Authentisierung
  - 16 Millionen Identitäten gestohlen (21.01.2014)
  - 18 Millionen Identitäten gestohlen (07.04.2014)
  - Heartbleed (11.04.2014)

# 16 Millionen Identitäten gestohlen (21.01.2014)

## Millionenfacher Identitätsdiebstahl: BSI bietet Sicherheitstest für E-Mail-Adressen

16 Millionen Digitale Identitäten betroffen

Bonn, 21.01.2014.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat angesichts eines Falles von großflächigem Identitätsdiebstahl unter <https://www.sicherheitstest.bsi.de> eine Webseite eingerichtet, auf der Bürgerinnen und Bürger überprüfen können, ob sie von diesem Identitätsdiebstahl betroffen sind. Im Rahmen der Analyse von Botnetzen durch Forschungseinrichtungen und Strafverfolgungsbehörden wurden rund 16 Millionen kompromittierte Benutzerkonten entdeckt. Diese bestehen in der Regel aus einem Benutzernamen in Form einer E-Mail-Adresse und einem Passwort. Viele Internetnutzer verwenden diese Login-Daten nicht nur für das eigene Mail-Account, sondern auch für Benutzerkonten bei Internetdiensten, Online-Shops oder Sozialen Netzwerken. Die E-Mail-Adressen wurden dem BSI übergeben, damit Betroffene informiert werden und erforderliche Schutzmaßnahmen treffen können.

Auf der Webseite <https://www.sicherheitstest.bsi.de>, die das BSI mit Unterstützung der Deutschen Telekom eingerichtet hat, können Internetnutzer ihre E-Mail-Adresse eingeben, um zu überprüfen, ob sie von dem Identitätsdiebstahl betroffen sind. Die eingegebene Adresse wird dann in einem technischen Verfahren vom BSI mit den Daten aus den Botnetzen abgeglichen. Ist die Adresse und damit auch die Digitale Identität des Nutzers betroffen, so erhält dieser eine entsprechende Information per E-Mail an die angegebene Adresse. Diese Antwort-Mail enthält auch Empfehlungen zu erforderlichen Schutzmaßnahmen. Ist die eingegebene E-Mail-Adresse nicht betroffen, so erhält der Nutzer keine Benachrichtigung.

# 18 Millionen Identitäten gestohlen (07.04.2014)

## Neuer Fall von großflächigem Identitätsdiebstahl: BSI informiert Betroffene

Bonn, 07.04.2014.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) informiert angesichts eines erneuten Falles von großflächigem Identitätsdiebstahl betroffene Bürgerinnen und Bürger in Deutschland. Die Staatsanwaltschaft Verden (Aller) hat dem BSI einen Datensatz mit rund 21 Millionen E-Mail-Adressen und Passwörtern zur Verfügung gestellt. Nach technischer Analyse und Bereinigung durch das BSI verblieben rund 18 Millionen von Identitätsdiebstahl betroffene E-Mail-Adressen, darunter rund 3 Millionen deutsche E-Mail-Adressen. Die Inhaber der E-Mail-Adressen werden vom BSI in Zusammenarbeit mit den Online-Dienstleistern Deutsche Telekom, Freenet, gmx.de, Kabel Deutschland, Vodafone und web.de informiert. Zudem stellt das BSI wieder einen webbasierten Sicherheitstest zur Verfügung.

Die digitalen Identitäten sind im Rahmen eines laufenden Ermittlungsverfahrens gefunden worden. Mit den E-Mail-Adressen und den zugehörigen Passwörtern versuchen Kriminelle mithilfe eines Botnetzes, sich in E-Mail-Accounts einzuloggen und diese für den Versand von SPAM-Mails zu missbrauchen. Das Botnetz ist noch in Betrieb, die gestohlenen Identitäten werden aktiv ausgenutzt. Es ist davon auszugehen, dass es sich bei den gefundenen Adressen und Passwörtern sowohl um Zugangsdaten zu E-Mail-Konten als auch um Zugangsdaten zu anderen Online-Accounts wie Online-Shops, Internet-Foren oder Sozialen Netzwerken handelt.

## BSI stuft "Heartbleed Bug" als kritisch ein

Bonn, 11.04.2014.

Der "Heartbleed-Bug", über den derzeit in den Medien berichtet wird, ist eine Sicherheitslücke in einer Programmiererweiterung von OpenSSL namens "Heartbeat". OpenSSL ist eine freie Software-Bibliothek für Transport Layer Security (TLS) und umfasst Implementierungen verschiedener Verschlüsselungen. Insbesondere Web- und Mail-Server aber auch andere Dienste wie Virtual Private Networks oder Appliances wie Router nutzen häufig diese Bibliothek für TLS/SSL-Verbindungen. Die Bibliothek enthält in den Versionen 1.0.1 bis 1.0.1f eine Schwachstelle, den "Heartbleed-Bug".

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stuft diese Schwachstelle als kritisch ein. Ein Angreifer ist unter Ausnutzung der Schwachstelle in der Lage, Speicherinhalte des OpenSSL Servers auszulesen, sofern diese die "Heartbeat"-Erweiterung aktiviert haben. Mithilfe des "Heartbleed Bugs" können zudem unter Umständen die geheimen Schlüssel von OpenSSL-Servern ausgelesen werden.

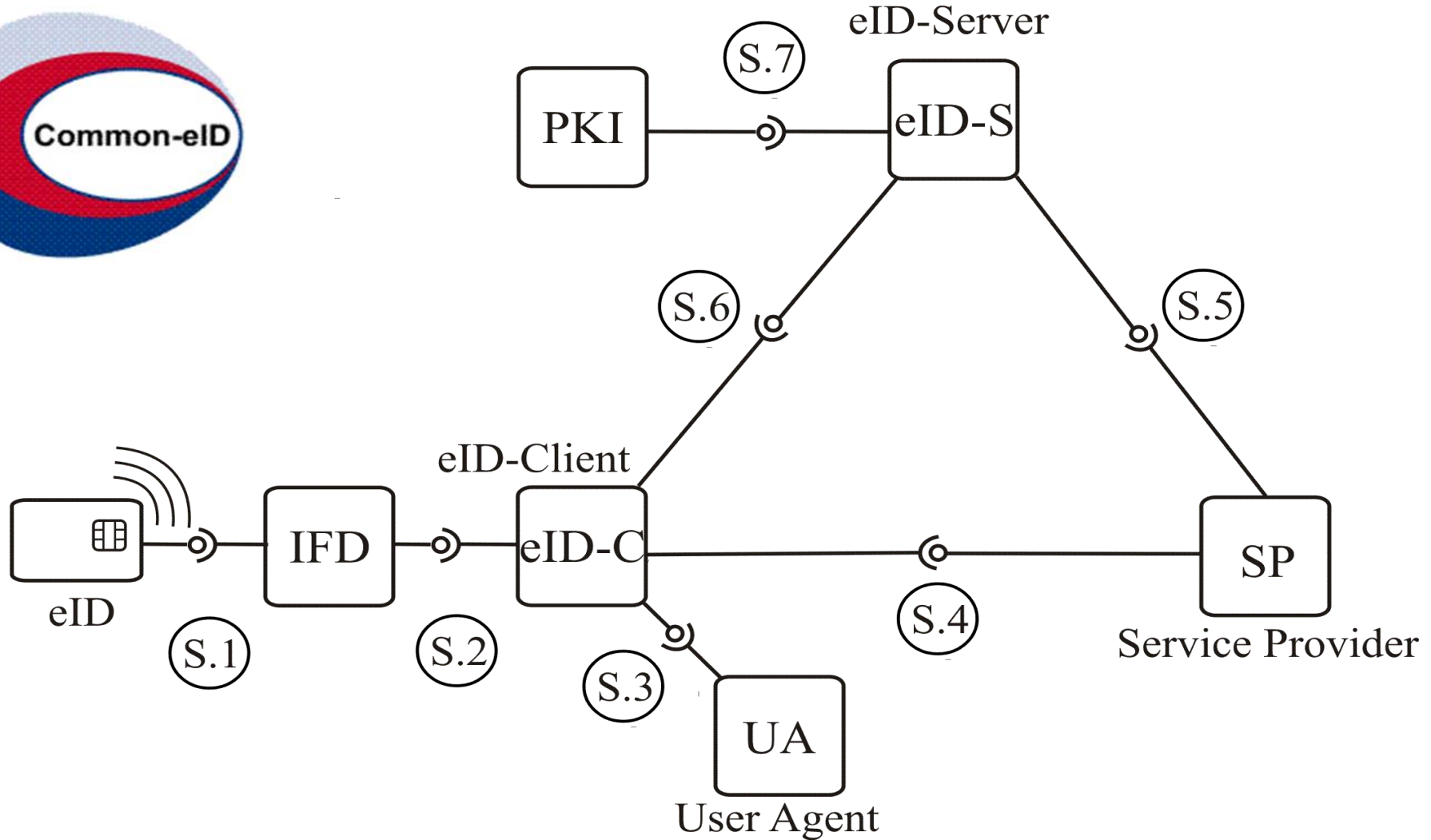
Seit dem 7. April 2014 steht mit OpenSSL Version 1.0.1g ein Update zur Verfügung, das die Sicherheitslücke schließt. Betreiber, die auf ihren Servern OpenSSL einsetzen, sollten das Update umgehend einspielen. Falls seit März 2012 eine verwundbare OpenSSL-Version mit aktivierter Heartbeat-Erweiterung eingesetzt wurde, kann eine vergangene Kompromittierung von Schlüsseln nicht ausgeschlossen werden. Daher empfiehlt das BSI in einem solchen Fall den Austausch der verwendeten OpenSSL Server-, beziehungsweise Client-Zertifikate und Schlüssel sowie eine Änderung der verwendeten Passwörter. Der Austausch sollte erst nach der Einspielung des Updates erfolgen, da ansonsten die neuen Zertifikate wieder kompromittiert werden könnten. Die alten Zertifikate müssen nach erfolgreichem Austausch gesperrt werden. Betreiber sind aufgerufen, ihre Nutzer über die Umsetzung der Aktualisierung zu informieren, damit diese ihre Passwörter kurzfristig ändern.

## Wo liegt das Problem?

- nPA-Zwischenbilanz nach 3,5 Jahren **eher ernüchternd**
  - existierende eID-Clients, eID-Server, eID-Services etc.
  - Anzahl an Diensteanbietern kaum steigend
  - kaum tatsächlich nutzbare Anwendungsdienste
- ... trotz des **sehr klaren** Bedarfs für starke Authentisierung
  - 16 Millionen Identitäten gestohlen (21.01.2014)
  - 18 Millionen Identitäten gestohlen (07.04.2014)
  - Heartbleed (11.04.2014)



# Unser eID-System





Hauptseite Meine Seite Projekte Administration Hilfe
Angemeldet als **detlef.huehnlein** Mein Konto Abmelden

## Common eID


Suche: 
Common eID ▾

Übersicht
Aktivität
Tickets
Neues Ticket
Gantt-Diagramm
Kalender
News
Dokumente
Wiki
Dateien
Konfiguration

### Übersicht + Neues Unterprojekt

Das reibungslose Zusammenwirken von verschiedenen Komponenten unterschiedlicher Hersteller in komplexen technischen Systemen ist bekanntlich mit vielfältigen Herausforderungen verbunden. Dies gilt insbesondere im Bereich der angewandten Kryptographie und im Bereich elektronischer Ausweise (eID).

Vor diesem Hintergrund zielt das Common eID Projekt darauf ab, die Interoperabilität im Umfeld des neuen Personalausweises durch geeignete Tests mit den verschiedenen Komponenten und Diensten der unterschiedlichen Anbieter zu steigern.



#### Tickets

- Bug: 7 offen / 7
- Feature: 0 offen / 0
- Support: 0 offen / 0
- Review: 1 offen / 1
- PartnerIssue: 3 offen / 3
- Suggestion: 3 offen / 3

#### Mitglieder

Manager: Detlef Hühnlein, Johannes Schmölz, Thomas Wieland, Tobias Wich

Member: Benedikt Biallowons, Hans-Martin Haase, Hartje Bruns, Max Tuengerthal

#### Aufgewendete Zeit

🕒 0.00 Stunde

[Details](#) | [Bericht](#)

# Common eID

Suche:  Common eID ▼

- Übersicht
- Aktivität
- Tickets**
- Neues Ticket
- Gantt-Diagramm
- Kalender
- News
- Dokumente
- Wiki
- Dateien
- Konfiguration

## Tickets

▼ Filter  
 Status  Filter hinzufügen

► Optionen

✓ Anwenden
↺ Zurücksetzen
💾 Speichern

✓ # ▼	Tracker	Status	Priorität	Thema	Zugewiesen an	Aktualisiert
<input type="checkbox"/> 296	Bug	New	Normal	Minor result code common#invalidChannelHandle missing in TR-03112-1		14.04.2014 18:07
<input type="checkbox"/> 295	Bug	New	Normal	Minor result code common#incorrectParameter missing in TR-03112-1		14.04.2014 16:23
<input type="checkbox"/> 288	Suggestion	New	Low	LegacySignatureGenerationInfo		01.04.2014 09:06
<input type="checkbox"/> 287	Suggestion	New	Normal	Corrigendum zum SignatureGenerationInfo vom 23.05.2011 sollte in TR-03112-4 eingearbeitet werden		01.04.2014 10:54
<input type="checkbox"/> 286	Bug	New	Normal	eCardServerAddress in UseIDResponse ist keine gültige URL		27.03.2014 15:48
<input type="checkbox"/> 285	Bug	New	Normal	Falsches ResultMajor Präfix		27.03.2014 15:32
<input type="checkbox"/> 284	Bug	New	Normal	Fehlende optionale Elemente in UseID Request erzeugen Fehler		27.03.2014 15:11
<input type="checkbox"/> 283	Suggestion	New	Normal	Expliziter Verweis auf WS-I Spezifikation in Kapitel 4 von BSI TR-03130-1		27.03.2014 14:35
<input type="checkbox"/> 282	Bug	New	Normal	Problem mit der Codierung des X509IssuerSerial-Elements		27.03.2014 14:28
<input type="checkbox"/> 203	Bug	New	Normal	Problem with Service of Tönjes		27.03.2014 14:59
<input type="checkbox"/> 201	PartnerIssue	New	Normal	Problem with Service of Teambank		27.03.2014 15:07
<input type="checkbox"/> 200	PartnerIssue	New	Normal	Problem with Service of Schufa		27.03.2014 14:55

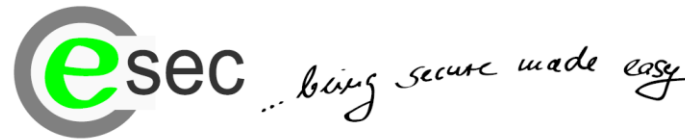
### Tickets

- [Alle Tickets anzeigen](#)
- [Zusammenfassung](#)
- [Kalender](#)
- [Gantt-Diagramm](#)

## Herzliche Einladung zur Mitwirkung

- Sie sind herzlich eingeladen,
  - am Common-eID-Projekt aktiv mitzuwirken,
  - die eID-Technologie interoperabel und leichter nutzbar zu machen,
  - die vertrauenswürdige Informations- und Kommunikationstechnik zu fördern und
  - schließlich das Internet und die Welt ein wenig sicherer zu machen!

# Herzlichen Dank für Ihre Aufmerksamkeit! ... Fragen?



**ecsec GmbH**

Sudetenstr. 16  
96247 Michelau, Germany  
Telefon + 49 9571 896479  
Mobil + 49 171 9754980  
detlef.huehnlein@ecsec.de  
<http://www.ecsec.de>

Dipl.-Inform. (FH)  
**Dr. Detlef Hühnlein**  
Geschäftsführer