**HIGH SEC MW eID EU**

**Përshkrimi i prodhimit**

**Version 2.1.1**

**Përmbajtja**

[Rreth prodhimit 3](#_Toc396932887)

[1 Hyrje 4](#_Toc396932888)

[2 Funksionalitetet i eID App 4](#_Toc396932889)

[3 Dokumentacioni për përdoruesin e fundit 4](#_Toc396932890)

[4 Sistemet operative të mbështetura 4](#_Toc396932891)

[5 Kartat smart të mbështetura 5](#_Toc396932892)

[6 Lexuesit e mbështetur të kartave smart 5](#_Toc396932893)

[7 Aplikacionet e mbështetura 5](#_Toc396932894)

[8 Third Party Software 6](#_Toc396932895)

[a. OpenSSL Toolkit 6](#_Toc396932896)

[OpenSSL License 6](#_Toc396932897)

[Original SSLeay License 7](#_Toc396932898)

[b. BouncyCastle Crypto APIs 8](#_Toc396932899)

[License 9](#_Toc396932900)

# Rreth prodhimit

HIGH SEC MW eID EU (eID App) është paketë softveri e destinuar për përmirsimin e sigurisë së aplikacioneve, të cilat mbshtesin PKCS#11 dhe CryptoAPI të Microsoft-it, me ndërmjetësinë e kartës smart. eID App përmban të gjithë funksionalitetin e domosdoshëm për përdorimin e kartave smart për enkripsionin, autentikacionin dhe nënshkrimin dixhital.

eID App mbështet kartat smart të personalizuara dhe të inicializuara StarCOS v3.5 (eID edicioni – si kontakte, ashtu edhe jokontakte) të zhvilluara nga ana e Giesecke & Devrient GmbH (G&D).

eID App vjen më paketën instaluese për sistemet operative: Windows XP/Vista/7/8/Server 2008 R2/2012.

Ekziston bashkësi e caktuar PC/SC të lexuesit të kartës smart, i cili mundet përdoret me eID App.

# Hyrje

SEC MW eID EU (HSMW), është pako softverike e destinuar për përsimin e sigurisë së aplikacioneve, të cilat mbështesin PKCS#11 dhe CryptoAPI të Microsoft-it me ndërmjetësinë e kartave smart. Paketa eID App përmban bibliotekën PKCS#11, furnizuesin e shërbimeve kriptografike (Cryptographic Service Provider, CSP), aplikacionin administrues, dhe servisin bazë. Paketa eID App mundëson përdorimin e informatave private dhe publike të vendosura në kartën smart. Sistemi mundet të përdori kartat smart për enkripsionin, autentikacionin dhe nënshkrimin dixhital.

# Funksionalitetet i eID App

eID App përmban të gjithë funksionalitetin e domosdoshëm për përdorimin e kartave smart në infrastrukturat e ndryshme të çelësit publik (Public Key Infrastructures, PKI). Kjo përfshin:

* CSP për integrimin e aplikacioneve të mbështetura në CryptoAPI të Microsoft-it (Internet Explorer, Microsoft Outlook, Adobe Acrobat)
* Biblioteka PKCS#11 për integrimin e aplikacioneve të mbështetura në PKCS#11 (MozillaFirefox, MozillaThunderbird, LotusNotes)
* Windows logon support
* Mbështetja për PC/SC v1.0
* Dokumentacioni për përdoruesin e fundit. Është përfshirë edhe dokumentacioni bazë për programuesit, i cili përmban përshkrim të shkurtër të funksioneve të implementuara
* Komplet paketa instaluese me mundësinë e zgjedhjes së komponentëve për instalimin
* Aplikacioni administrativ për vizualizimin dhe administrimin e kartës smart.

# Dokumentacioni për përdoruesin e fundit

eID App vjen me dokumentacionin e mëposhtëm për përdoruesin e fundit dhe dokumentacionin për programuesit:

* Udhëzime për instalimin eID App
* Udhëzime për përdorimin për Aplikacionin administrator
* Përshkrimi i CSP-së
* Përshkrimi i bibliotekës PKCS#11

# Sistemet operative të mbështetura

eID App është testuar dhe mbështetur në sistemet operative të mëposhtëme:

* Microsoft Windows XP 32-bit
* Microsoft Windows Vista 32-bit/64-bit
* Microsoft Windows 7 32-bit/64-bit
* Microsoft Windows 8 32-bit/64-bit
* Microsoft Windows Server 2008 R2 64-bit
* Microsoft Windows Server 2012 64-bit

# Kartat smart të mbështetura

eID App është destinuar për përdorimin me StarCOS v3.5 të kartës smart (edicioni eID – si për kontakte, ashtu dhe ato jokontakte), të zhvilluar nga ana e Giesecke & Devrient GmbH.

# Lexuesit e mbështetur të kartave smart

eID App mundet të përdoret me lexuesit e kartave smart, të cilat kanë i interfejs PC/SC. Lexuesit e mëposhtëm të kartave smart janë testuar:

* HID Omnikey 3121(i njohur edhe si CardMan 3121)
* HID Omnikey 5321 v2
* HID Omnikey 5321 v2 jokontakte
* SCM SDI 011 jokontakte
* Tastiera Cherry G83-6644 me lexuesin e integruar të kartës smart

# Aplikacionet e mbështetura

Lista e mëposhtëme përmban aplikacione, të cilat janë të testuara dhe që eID App i mbështet. Lista nuk është gjithëpërfshirëse, dhe ekziston mundësia e madhe që edhe aplikacionet e tjera, të cilat punojnë me CryptoAPI dhe/ose me bibliotekat PKCS#11, mundet të përdorin me sukses serviset, të cilat i ofron eID App:

|  |  |
| --- | --- |
| **Aplikacioni** | Microsoft Internet Explorer |
| **Verzioni i Aplikacionit** | 6, 7, 8, 9 dhe 10 |
| **Përshkrimi** | Autentikacioni i përdoruesit i bazuar në çertifikatat dixhitale |
| **API** | CryptoAPI (CSP) |

|  |  |
| --- | --- |
| **Aplikacioni** | Mozilla Firefox |
| **Verzioni i Aplikacionit** | Të gjitha versionet të përfunduara me 24 |
| **Përshkrimi** | Verifikimi i përdoruesit i bazuar në çertifikatat digjitale. |
| **API** | PKCS#11 |

|  |  |
| --- | --- |
| **Aplikacioni** | Microsoft Word |
| **Verzioni i Aplikacionit** | 10, 11, 2007 dhe 2010 |
| **Përshkrimi** | Mbrojtja e integritetit, pakthyeshmërisë dhe autenticionit të dokumentave |
| **API** | Crypto API (CSP) |

|  |  |
| --- | --- |
| **Aplikacioni** | Microsoft Outlook |
| **Verzioni i Aplikacionit** | Express 6, Mail 1.0. Live Mail 2011, 11, 12 dhe 14 |
| **Përshkrimi** | Mbrojtja e integritetit, pakthyeshmërisë dhe autenticionit të postës elektronike |
| **API** | CryptoAPI (CSP) |

|  |  |
| --- | --- |
| **Aplikacioni** | Mozilla Thunderbird |
| **Verzioni i Aplikacionit** | Të gjitha versionet të përfunduara me 24 |
| **Përshkrimi** | Mbrojtja e integritetit, pakthyeshmërisë dhe autenticionit të postës elektronike |
| **API** | PKCS#11 |

|  |  |
| --- | --- |
| **Application** | Adobe Acrobat |
| **Verzioni i Aplikacionit** | Standard 8, 9 dhe 10 |
| **Përshkrimi** | Mbrojtja e integritetit, pakthyeshmërisë dhe autenticionit të dokumentave |
| **API** | CryptoAPI (CSP) |

|  |  |
| --- | --- |
| **Application** | Lotus Notes |
| **Verzioni i Aplikacionit** | 7 dhe 8.5 |
| **Përshkrimi** | Mbrojtja e integritetit, pakthyeshmërisë dhe autenticionit të postës elektronike |
| **API** | PKCS#11 |

|  |  |
| --- | --- |
| **Application** | PGP Desktop |
| **Verzioni i Aplikacionit** | 9.10 dhe 10 |
| **Përshkrimi** | Mbrojtja e integritetit, pakthyeshmërisë dhe autenticionit të datotekës |
| **API** | PKCS#11 |

|  |  |
| --- | --- |
| **Application** | Google Chrome |
| **Verzioni i Aplikacionit** | Nga 25 deri në 30 |
| **Përshkrimi** | Autentikacioni i përdoruesit i bazuar në çertifikatat dixhitale |
| **API** | CryptoAPI (CSP) |

# Third Party Software

The HIGHSEC eID App installation package contains software developed by third parties:

## OpenSSL Toolkit

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com). The usage of the OpenSSL Toolkit is provided under the license conditions as stated here: <http://www.openssl.org/source/license.html>.

### OpenSSL License

Copyright (c) 1998-2011 The OpenSSL Project.  All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

1. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
2. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
3. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to.  The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

1. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed.  i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

## BouncyCastle Crypto APIs

This product includes software developed by the Legon of Bouncy Castle [http://www.bouncycastle.org](http://www.bouncycastle.org/).

The usage of the BouncyCastle Crypto API is provided under the license terms as stated here: <http://bouncycastle.org/licence.html>

Please note this should be read in the same way as the [MIT license](http://opensource.org/licenses/MIT).

### License

Copyright (c) 2000 - 2013 The Legion of the Bouncy Castle Inc. ([http://www.bouncycastle.org](http://www.bouncycastle.org/))

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.