



Zentrum für sichere Informationstechnologie – Austria Secure Information Technology Center – Austria

A-1040 Wien, Weyringergasse 35
Tel.: (+43 1) 503 19 63-0
Fax: (+43 1) 503 19 63-66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

<http://www.a-sit.at>
E-Mail: office@a-sit.at

REMOTE SECUREEFS BÜRGERKARTE VERSION 1.0, 15.11.2007

DI Arne Tauber – arne.tauber@a-sit.at

1 **Zusammenfassung:** EFS (Encrypting File System) wird von Microsoft als integraler Bestandteil
2 des Betriebssystems ab der Version Windows 2000 mitgeliefert.

3
4 Im Unterschied zur Auslieferungsversion des Herstellers werden mit Hilfe von SecureEFS die EFS-
5 Schlüssel dem Betriebssystem nur während des Anmeldevorgangs zur Verfügung gestellt und
6 dann sicher gelöscht. Damit wird sichergestellt, dass die Daten nur von ordnungsgemäß
7 angemeldeten Benutzern entschlüsselt werden können, nicht jedoch im Falle von Verlust oder
8 Diebstahl (z.B. von Laptops).

9
10 Dieses Dokument beschreibt den Betrieb einer SecureEFS [SecureEFS] Installation mit einer
11 Bürgerkartenumgebung [BKU], welche nicht lokal, sondern remote (bspw. zentral in einem
12 Intranet) installiert ist.

13

Inhaltsverzeichnis

| | |
|---------------------------------------|----|
| Inhaltsverzeichnis | 1 |
| Abbildungsverzeichnis | 2 |
| Begriffsdefinition | 3 |
| 1 Einleitung | 4 |
| 1.1 Ziele | 4 |
| 1.2 Anwendungsbereich | 4 |
| 1.2.1 Schutz..... | 4 |
| 1.3 Voraussetzungen | 5 |
| 1.4 SecureEFS und Windows Vista | 5 |
| 2 Konfiguration..... | 6 |
| 2.1 Beispielinstallation | 6 |
| Referenzen | 9 |
| Historie | 10 |

Abbildungsverzeichnis

| | |
|--|---|
| Abbildung 1: Konfiguration einer Remote SecureEFS Installation | 6 |
| Abbildung 2: SecureEFS Optionen | 7 |

Dieses Dokument verwendet die Schlüsselwörter MUSS, DARF NICHT, ERFORDERLICH, SOLLTE, SOLLTE NICHT, EMPFOHLEN, DARF, und OPTIONAL zur Kategorisierung der Anforderungen. Diese Schlüsselwörter sind analog zu ihren englischsprachigen Entsprechungen MUST, MUST NOT, REQUIRED, SHOULD, SHOULD NOT, RECOMMENDED, MAY, und OPTIONAL zu handhaben, deren Interpretation in RFC 2119 festgelegt ist.

Begriffsdefinition

14 **Bürgerkarte:** Laut [E-GovG], §10 ZI 10 ist die Bürgerkarte "die unabhängig von der Umsetzung
15 auf unterschiedlichen technischen Komponenten gebildete logische Einheit, die eine elektronische
16 Signatur mit einer Personenbindung (§ 4 Abs. 2) und den zugehörigen Sicherheitsdaten und –
17 funktionen sowie mit allenfalls vorhandenen Vollmachtsdaten verbindet". Im Sinne der in den
18 Spezifikationen zur österreichischen Bürgerkarte gebrauchten Terminologie ist die Bürgerkarten-
19 Umgebung die Implementierung der logischen Einheit Bürgerkarte.

20 **Bürgerkartenumgebung:** Jenes Programm bzw. jener Dienst, der die Funktionalität der
21 Bürgerkarte zur Verfügung stellt. Grundsätzlich vorstellbar ist die Ausführung als Programm, das
22 lokal am Rechner des Bürgers läuft (lokale Bürgerkarten-Umgebung), oder als serverbasierter
23 Dienst, der über das Internet angesprochen wird (serverbasierte Bürgerkarten-Umgebung). Die
24 Interaktion mit diesem Programm bzw. Dienst wird über zwei Schnittstellen abgewickelt: Über die
25 Benutzer-Schnittstelle sowie über den Security-Layer.

26 **SecureEFS:** Im Unterschied zur Auslieferungsversion des Herstellers werden mit Hilfe von
27 SecureEFS die EFS-Schlüssel dem Betriebssystem nur während des Anmeldevorgangs zur
28 Verfügung gestellt und dann sicher gelöscht. Damit wird sichergestellt, dass die Daten nur von
29 ordnungsgemäß angemeldeten Benutzern entschlüsselt werden können, nicht jedoch im Falle von
30 Verlust oder Diebstahl (z.B. von Laptops).

1 Einleitung

31 EFS (Encrypting File System) wird von Microsoft als integraler Bestandteil des Betriebssystems ab
32 der Version Windows 2000 mitgeliefert.

33
34 Im Unterschied zur Auslieferungsversion des Herstellers werden mit Hilfe von SecureEFS die EFS-
35 Schlüssel dem Betriebssystem nur während des Anmeldevorgangs zur Verfügung gestellt und
36 dann sicher gelöscht. Damit wird sichergestellt, dass die Daten nur von ordnungsgemäß
37 angemeldeten Benutzern entschlüsselt werden können, nicht jedoch im Falle von Verlust oder
38 Diebstahl (z.B. von Laptops).

39
40 Dieses Dokument beschreibt den Betrieb einer SecureEFS [SecureEFS] Installation mit einer
41 Bürgerkartenumgebung [BKU], welche nicht lokal, sondern remote (bspw. zentral in einem
42 Intranet) installiert ist.

1.1 Ziele

43 Die wesentlichen Ziele und Vorteile einer derartigen Installationsvariante sind wie folgt:

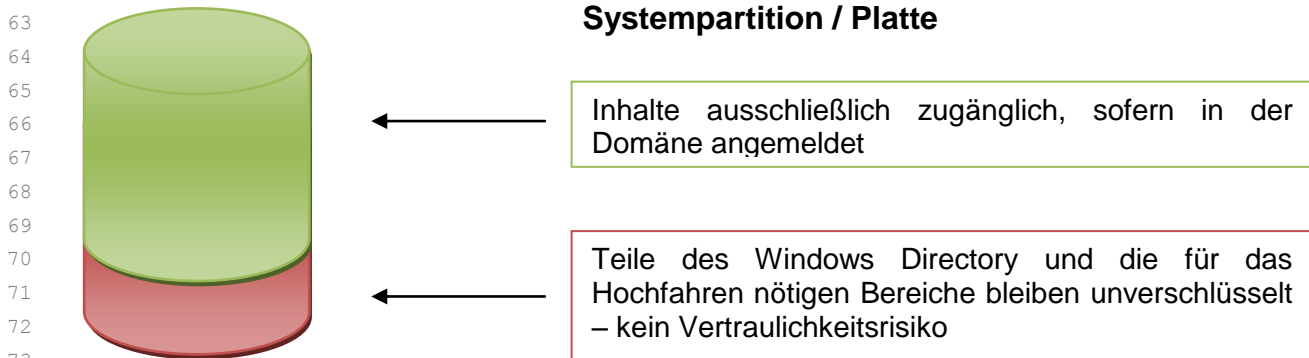
- 44
45 • Plattenbereiche von Desktoprechnern in einem lokalen Netzwerk können mit einem
46 zentralen Schlüssel auf einer einzigen Karte abgesichert werden. Das Verwalten von
47 einzelnen Karten ist somit nicht mehr notwendig und reduziert erheblich die
48 Ausfallsicherheit.
- 49
50 • Sofern der Rechner nicht in der Domäne gestartet wird, verbleiben die betroffenen
51 Plattenbereiche stark verschlüsselt (AES). Bei Rechnertausch, Reparatur bzw. Diebstahl
52 können die verschlüsselten Bereiche nicht ausgelesen werden.

1.2 Anwendungsbereich

53 Die in diesem Dokument beschriebene Betriebsvariante zielt in erster Linie auf Desktoprechner ab,
54 welche einen persistenten Zugang zum zentralen Rechner mit der darauf installierten und
55 laufenden Bürgerkartenumgebung Zugriff haben. Für mobile Geräte wie Laptops, welche nicht
56 immer Zugriff auf das Intranet und somit auf die Bürgerkartenumgebung haben, wird eine
57 SecureEFS Installation mit einer eigenen Bürgerkarte empfohlen.

58
59 Die hier beschriebene Variante zielt hauptsächlich auf den Einsatz in einem abgegrenzten Bereich
60 (bspw. Intranet) ab. Beim Einsatz (z.B. in einem Kabinett) kann die Bürgerkartenumgebung auch
61 auf einem Rechner (z.B. Sekretariatsrechner) laufen und somit der Zugriff temporär deaktiviert
62 werden.

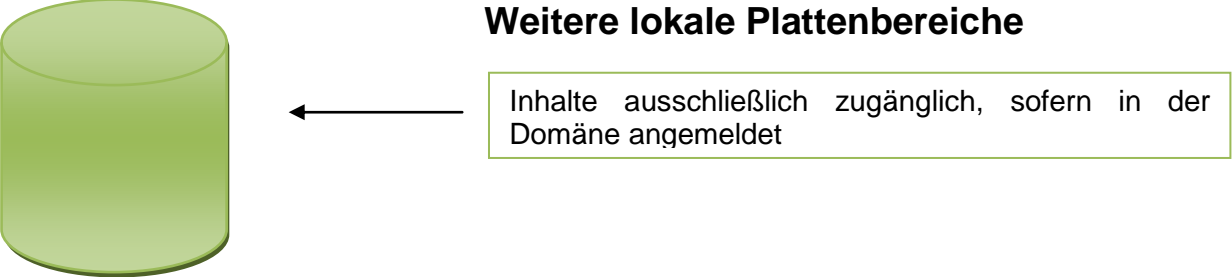
1.2.1 Schutz



76 Jene Teile, welche auf der Systempartition für das Hochfahren und Starten von Windows benötigt
77 werden, müssen unverschlüsselt bleiben. Diese Teile stellen jedoch kein Vertraulichkeitsrisiko dar.
78 Alle anderen Daten auf der Systempartition können verschlüsselt werden, da auf diese erst nach
79 dem Hochfahren des Systems und der Freischaltung über SecureEFS zugegriffen wird.
80

81 **Hinweis:** alle Programme, die automatisch mit Windows gestartet werden, müssen unverschlüsselt
82 bleiben, da erst nach dem Freischalten über SecureEFS verschlüsselte Bereiche der Festplatte
83 zugänglich werden.
84

85
86 **Weitere lokale Plattenbereiche**

87 88 Inhalte ausschließlich zugänglich, sofern in der
89 Domäne angemeldet
90
91
92

1.3 Voraussetzungen

93 Für den Betrieb einer Remote SecureEFS Installation sind folgende Voraussetzungen notwendig:
94

Lokaler Rechner

- 95 ○ Installation von SecureEFS (mind. Version 1.2)

Zentraler Rechner

- 96 ○ Bürgerkartenumgebung mit Unterstützung für XML Encryption (Security Layer 1.2)
- 97 ○ Port Forwarding Tool

98
99
100
101 Für den Betrieb von SecureEFS wird eine Bürgerkartenumgebung vorausgesetzt, welche XML
102 Encryption unterstützt. Daher muss die Bürgerkartenumgebung spezifikationsgemäß die
103 SecurityLayer Schnittstelle 1.2 implementieren. Als Beispiel für eine für SecureEFS taugliche
104 Bürgerkartenumgebung sei hier die Middleware trustDesk Basic der Fa. IT-Solution genannt,
105 welche diese Funktion unterstützt.
106
107
108

109 Ein Port Forwarding Tool ist notwendig, da die meisten Bürgerkartenumgebungen nur
110 Verbindungen vom gleichen Rechner aus zulassen. Um nun eine remote Verbindung als lokale
111 Verbindung zu „maskieren“ muss ein solches Tool am zentralen Rechner installiert werden.
112

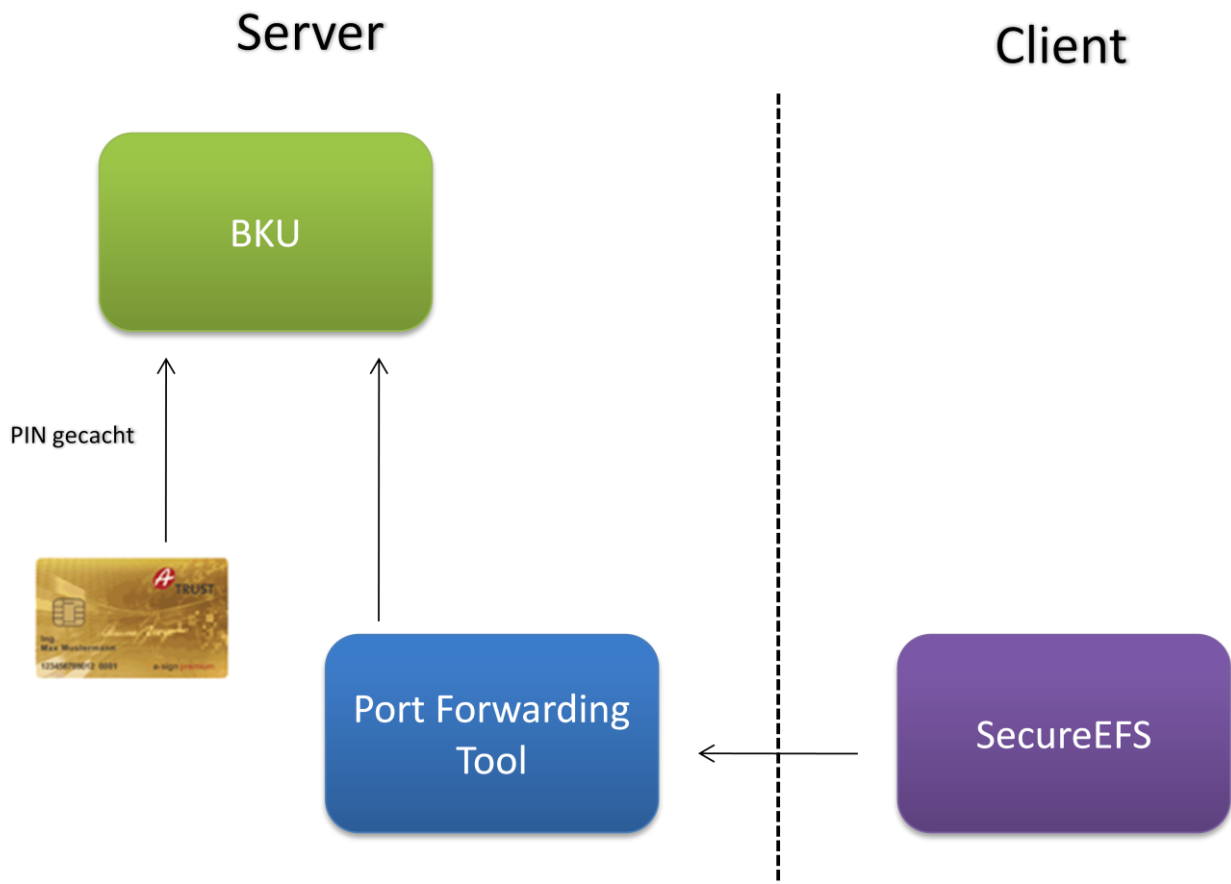
1.4 SecureEFS und Windows Vista

113 SecureEFS ist ausschließlich unter Windows XP und Windows 2000 lauffähig. Eine Unterstützung
114 für Windows Vista ist nicht gegeben. Jedoch bietet EFS ab Vista eine Unterstützung von
115 Smartcards an¹, sodaß private EFS Keys auch stark verschlüsselt im Dateisystem abgelegt
116 werden können.
117

¹ <http://www.microsoft.com/technet/technetmag/issues/2006/05/FirstLook/>

2 Konfiguration

118 Die Konfiguration einer Remote SecureEFS Umgebung sieht wie folgt aus:
119



120
121
Abbildung 1: Konfiguration einer Remote SecureEFS Installation

122
123
124 Auf dem zentralen Server wird eine Bürgerkartenumgebung installiert und die Bürgerkarte
125 eingesteckt. Die Geheimhaltungs-PIN wird in der Bürgerkartenumgebung gecached, sodass für
126 den Entschlüsselungsvorgang des privaten EFS-Schlüssels diese nicht manuell eingegeben
127 werden muss. Es wird empfohlen, eine oder zwei zusätzliche Ersatzkarten zu installieren und die
128 PINs dazu ebenfalls zu cachen. Diese Karten müssen entsprechend gesichert (Safe o.ä.)
129 aufbewahrt werden. Im Falle des Ausfalls einer Karte können dann die zusätzlichen Karten für den
130 aufrechten Betrieb von Remote SecureEFS verwendet werden.

131
132 Zusätzlich zur Bürgerkartenumgebung wird ein Port Forwarding Tool installiert, das externe
133 Verbindungen auf einen beliebigen Port (HTTP) an die Bürgerkartenumgebung weiterleitet. Das
134 Tool muss jedoch so installiert werden, dass die Remote Adresse der Verbindung versteckt wird,
135 und eine lokale Verbindung an die Bürgerkartenumgebung emuliert wird. Das Port Forwarding Tool
136 darf ausschließlich vom internen Netz oder von dedizierten Rechnern aus zugänglich sein.

137
138 SecureEFS wird so konfiguriert, dass in der Adresszeile der Bürgerkartenumgebung nicht
139 „localhost“, sondern die IP-Adresse oder der Hostname des Servers eingegeben wird.

2.1 Beispielininstallation

140 Dieser Abschnitt beschreibt eine beispielhafte Installation von Remote SecureEFS mit der
141 entsprechenden Konfiguration und den verwendeten Softwarekomponenten.

142

143 Verwendete Software am Server:

- 144
- 145 • Bürgerkartenumgebung: trustDesk basic 2.7.7
- 146 • Port Forwarding Tool: IAIK Proxy Tunnel 1.8 Client (JDK 1.4 Version)
- 147

148 Verwendete Bürgerkarte: aktivierte e-Card
149 Kartenleser: Gemplus GemPC USB-SL

150
151 Nachfolgend die Konfigurationsdatei des IAIK Proxy Tunnels Client:

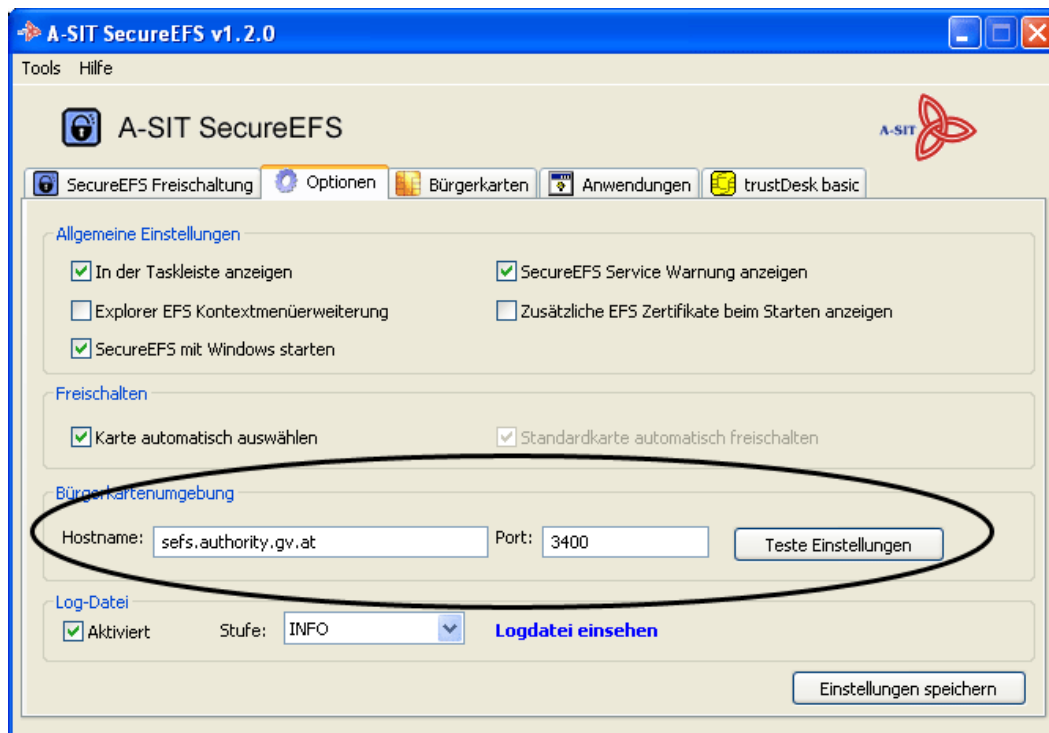
```
152  
153 NumTunnels=1  
154 Tunnel.1=REMOTE_BKU_SEFS  
155 CipherSuite = *aes *strong  
156 LogFile=client.log  
157 AccessLog = clientaccess.log  
158 connectHost=localhost  
159 REMOTE_BKU_SEFS.InPort = 3400  
160 REMOTE_BKU_SEFS.OutPort = 3495  
161 REMOTE_BKU_SEFS.OutputUsesSSL = false  
162 REMOTE_BKU_SEFS.connectHost=localhost
```

163
164 Das Starten des Proxy Tunnels Client wird über einen Eintrag im Autostart Menü von Windows
165 über den Link zur Datei runclient-silent.bat empfohlen. Der externe Port muss in diesem Fall ein
166 unterschiedlicher sein, da hier kein „echtes“ Portforwarding durchgeführt wird, sondern ein Tunneln
167 der Daten vom externen Port auf den internen Port der Bürgerkartenumgebung (3495). Als
168 externer Port wird hier der Wert 3400 verwendet, es kann jedoch auch jede beliebige andere freie
169 Portnummer verwendet werden.

170
171 Die BKU Einstellungen der SecureEFS Konfiguration müssen wie folgt sein:

172 Hostname/IP-Adresse: entspricht der des zentralen Rechners mit BKU Installation
173 Port: 3400

176



177

178

Abbildung 2: SecureEFS Optionen

179

180 SecureEFS kann nun wie üblich verwendet werden, ohne dass jedoch lokal eine Bürgerkarte
181 eingesteckt ist. Die Aktivierung und Verwendung von SecureEFS ist nun ident der lokalen
182 Installation einer Bürgerkarte. Weiterführende Informationen dazu gibt es in der Dokumentation
183 [SecureEFS].
184

Referenzen

| | |
|-------------|--|
| [BKU] | Hollosi A., Karlinger G., Einführung in die österreichische Bürgerkarte. Abgerufen am 15.11.2007 unter http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/introduction/Introduction.html |
| [SecureEFS] | Tauber A., SecureEFS Dokumentation. Abgerufen am 15.11.2007 unter http://demo.a-sit.at/buergerkarte/secure_efs/resources/SecureEFS.chm |

Historie

| | | |
|------------------------------------|----------------------------|----------------------------------|
| Version 1.0 | Datum 15.11.2007 | Kommentar Erstversion. |
| Ersteller DI Arne Tauber | | |