A-Trust Gesellschaft für Sicherheitssysteme
im elektronischen Datenverkehr GmbH
Landstraßer Hauptstraße 5
Tel: +43 (1) 713 21 51 - 0
Fax: +43 (1) 713 21 51 - 350
https://www.a-trust.at

a.sign Client
Installation Guide

Version: 3.1
Datum: 16. November 2023

Inhaltsverzeichnis

1 Aufbau und Komponenten **3**

1.1 Microsoft Cryptographic Service Provider (CSP) . . . 3

1.2 PKCS#11 Schnittstelle . . . 4

1.3 Kartenverwaltung . . . 5

1.4 Administrative Funktionen . . . 6

2 Lokale Installation **7**

3 Installation ohne Benutzerinteraktion (Silent) **10**

4 Installation für Card Registration System (CRS) **11**

5 Installation für Windows-Domain Login mit Signaturkarte **12**

6 Vorkonfigurieren der Kartenleser **13**

6.1 Kartenleser-Konfiguration vorbereiten . . . 13

6.2 Einstellungen exportieren . . . 13

6.3 Zusammenfassten von Einträgen . . . 14

6.4 Installieren der REG-Dateien auf den Zielsystem . . . 14

7 Installationsparameter **15**

7.1 Silent /S . . . 15

7.2 Installationsverzeichnis /D= . . . 15

7.3 Deaktivieren des CRC Check /NCRC . . . 15

7.4 CRS Installation /CRS=YES . . . 15

7.5 Automatische Updates /UPDATEABLE=NO . . . 15

7.6 Kartenlesereinstellungen behalten /KeepReaders . . . 16

7.7 A-Trust Reparatur Programm deaktivieren /FixIt=NO . . . 16

8 Registry Einträge **17**

8.1 Registry Einträge für Microsoft CSP (MiniTreiber) . . . 17

8.1.1 Arbeitsplatz Einstellungen . . . 17

8.1.2 Benutzer Einstellungen 18
8.2 Registry Enträge für PKCS#11 Schnittstelle 18
8.2.1 Arbeitsplatz Einstellungen 18
8.2.2 Benutzereinstellungen Einstellungen 20
8.3 Registry Enträge für Applikationen 20
8.4 Mini Treiber PIN Cache Policy 21

9 Installationshinweis **23**
9.1 Installation Microsoft CSP 23
9.2 USB Kartenleser - Kartenleser wird von Windows abgeschalten 23
9.3 Domain Anmeldeprobleme nach Neustart bei langsamen Verbindungen . 24

1 Aufbau und Komponenten

Der a.sign Client stellt die Schnittstelle zwischen Signaturkarte und Standard-Programmen dar. Um kryptografische Funktionen wie Signatur und Verschlüsselung bereitzustellen sind folgende Schnittstellen implementiert:

- Microsoft Cryptographic Service Provider (CSP), durch das Microsoft MiniTreiber Konzept
- PKCS#11 Schnittstelle

Zusätzlich sind Programme zum Verwalten der Signaturkarte im a.sign Client enthalten.

- Kartenverwaltung
- Administrative Funktionen

1.1 Microsoft Cryptographic Service Provider (CSP)

Der Cryptographic Service Provider[1] (CSP) ist eine von Microsoft definierte Schnittstelle welche vorallem für die Verwendung der Signaturkarte in Microsoft Funktionen benötigt wird. Auch einige Drittanbieter Programme verwenden diese Schnittstelle (z.B.: Google Chrome).

Der CSP wird beispielsweise von folgenden Produkten benötigt:

- Microsoft ®Internet Explorer / Outlook Express ab Version 5.x
- Microsoft ®Outlook
- Microsoft ®Office
- Google Chrome
- Adobe ®Acrobat ab Version 6

Der Cryptographic Service Provider wird durch das mit Windows Vista eingeführte MiniTreiber Konzept[2] implementiert.

[1] http://msdn.microsoft.com/en-us/library/windows/desktop/aa380245(v=vs.85).aspx
[2] http://msdn.microsoft.com/en-us/library/windows/hardware/gg487500.aspx

1.2 PKCS#11 Schnittstelle

PKCS#11[3] ist eine Schnittstelle für den Zugriff auf Signaturkarten welche Platformübergreifend verfügbar ist. Der PKCS#11 Standard definiert eine Programm-Schnittstelle für den Zugriff auf kryptografische Informationen und Funktionen[4].

Diese Schnittstelle wird beispielsweise von folgenden Produkten benötigt:

- Mozilla Thunderbird ®
- Mozilla Firefox ®
- Apache Open Office ™
- LibreOffice

[3] Public-Key Cryptography Standards - Cryptographic Token Interface Standard
[4] http://www.rsa.com/rsalabs/node.asp?id=2133

1.3 Kartenverwaltung

Dieses Programm zur Verwaltung der Signaturkarte. Damit können die Zertifikate der Karte ausgelesen werden, die Signatur-PIN geändert und entsperrt werden. Zu Testzwecken kann eine Signatur über Testdaten durchgeführt werden. Mit diesem Programm kann man auch die Infobox anzeigen lassen und ablaufende Zertifikate verlängern.

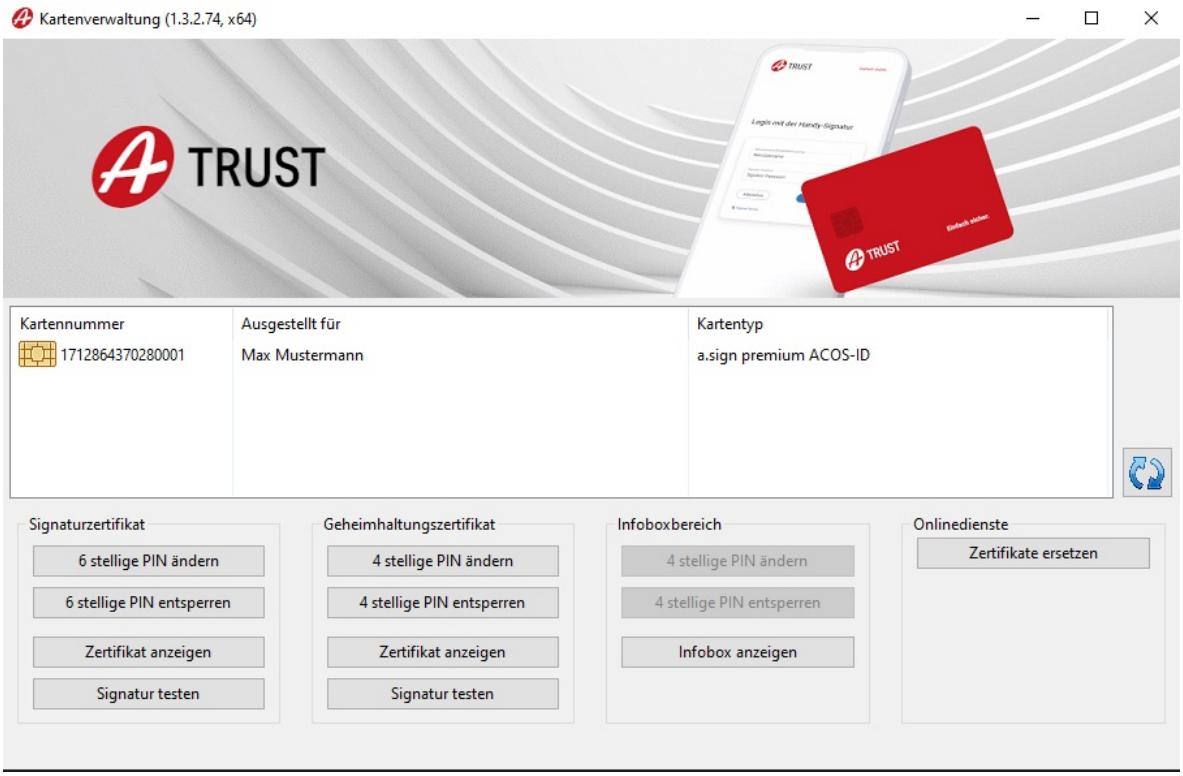

Abbildung 1: Kartenverwaltung

1.4 Administrative Funktionen

Dieses Programm dient zur Konfiguration und Verwaltung der a.sign Client Installation. Damit können die verwendeten Kartenleser eingeschränkt werden, sowie Logging und Diagnose Funktionen ausgeführt werden.

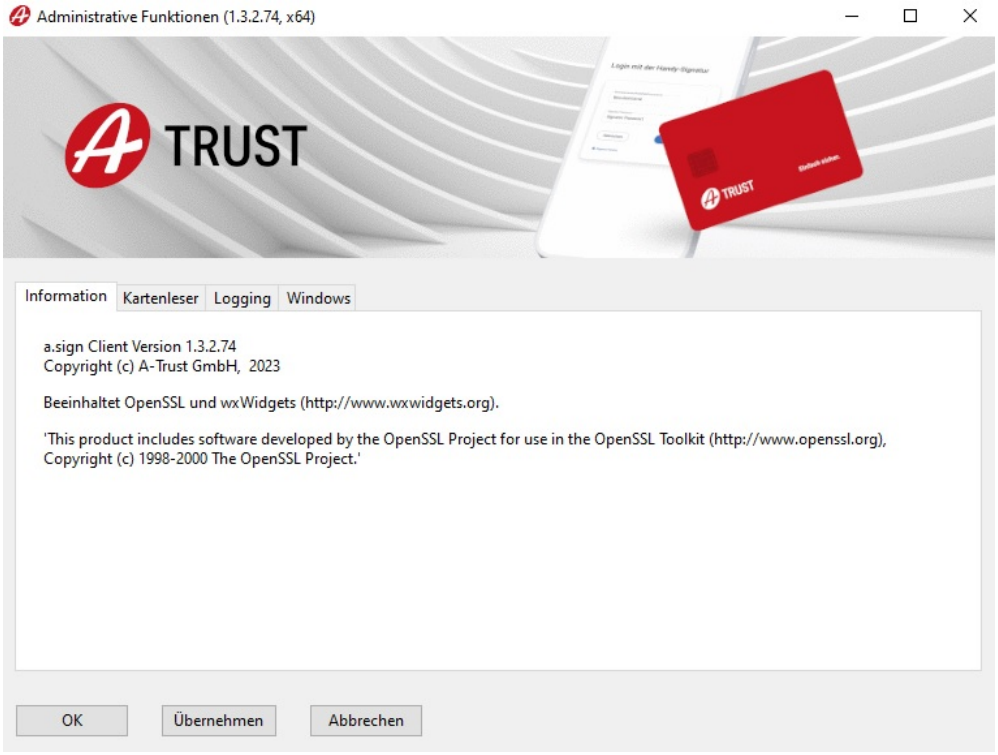

Abbildung 2: Administrative Funktionen

2 Lokale Installation

Nach dem Start des Setup des a.sign Clients erscheint der Wilkommensbildschirm. Mit der `Weiter` Schaltfläche gelangen Sie auf die nächste Seite.

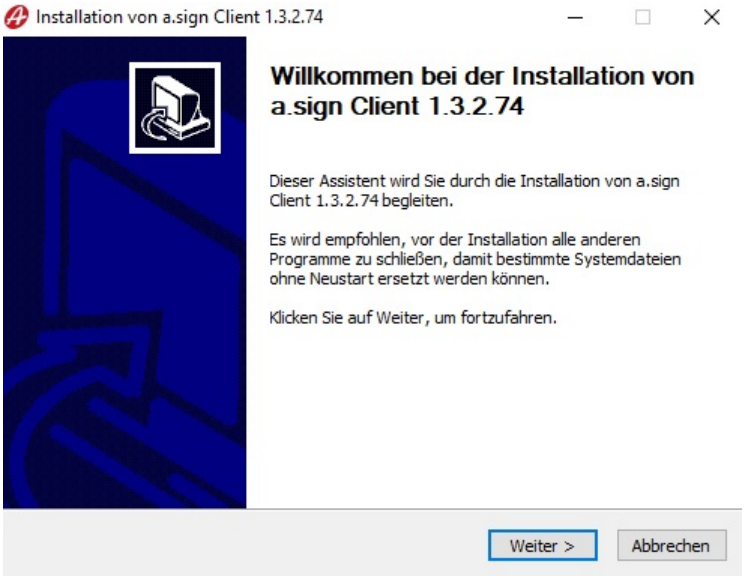

Abbildung 3: Installation Willommensbildschirm

Auf der zweiten Seite wird das Lizenzabkommen angezeigt. Bitte lesen Sie dieses sorgfältig durch! Mit der Schaltfläche `Annehmen` setzen Sie die Installation fort.

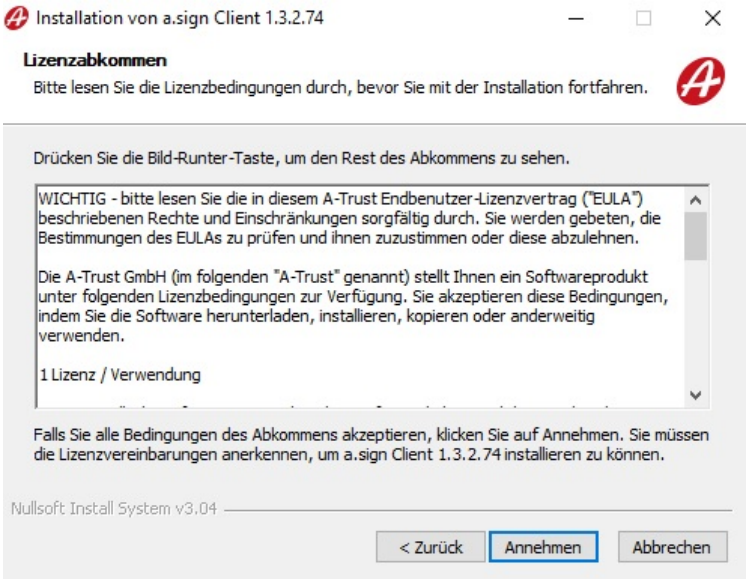

Abbildung 4: Installation Lizenz

Auf der dritten Seite können Sie sich das Installationsverzeichnis für den a.sign Client aussuchen. Wir empfehlen hier das vorgeschlagene Verzeichnis beizubehalten und über die Schaltfläche `Installieren` die Installation zu starten.

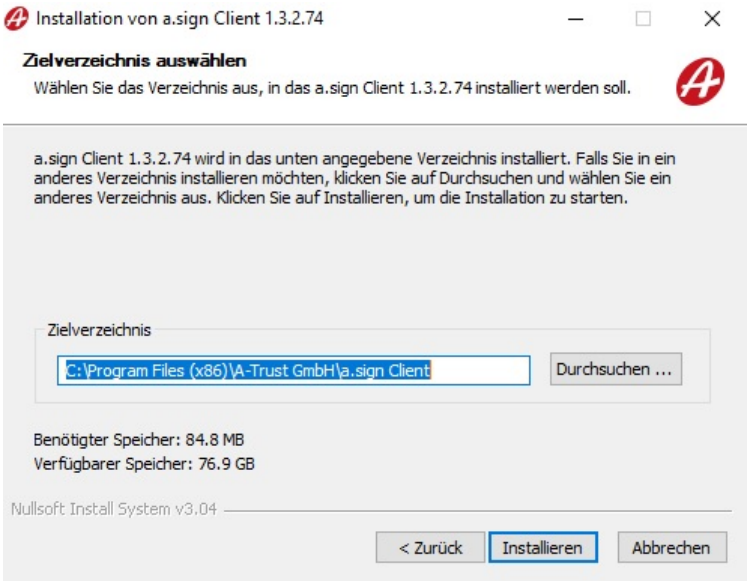

Abbildung 5: Installation Verzeichnis

Anschließend startet der Installationsvorgang, dies kann abhängig von Ihrem Computer bis zu einigen Minuten dauern.

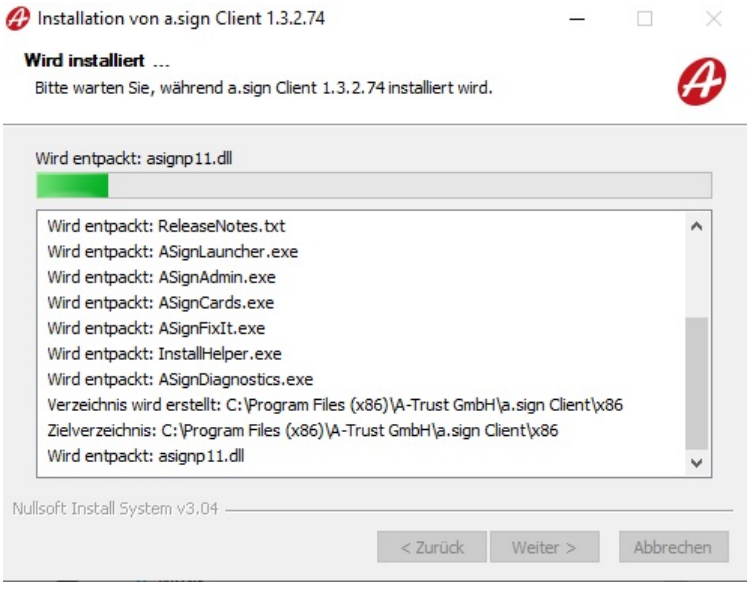

Abbildung 6: Installationsvorgang

Nach dem Installationsvorgang wird die Abschlußseite angezeigt, hier können Sie die installierte Software automatisch starten.

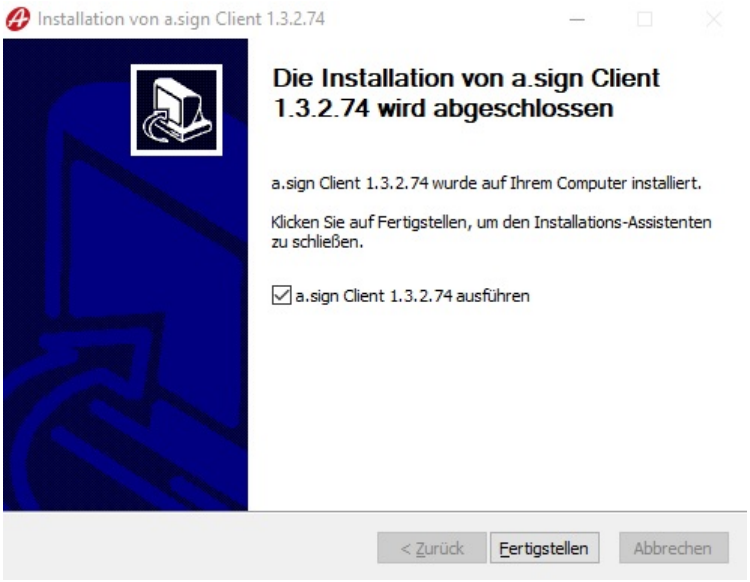

Abbildung 7: Abschlußseite

3 Installation ohne Benutzerinteraktion (Silent)

Um das Setup des a.sign Client ohne Benutzerinteraktion zu starten kann der Parameter /S verwendet werden.

```
ASignClient_v1.3.2.74_Setup.exe /S
```

4 Installation für Card Registration System (CRS)

Wenn die Software für das CRS installiert werden soll, dann verwenden Sie bitte den Parameter `/CRS=Yes`. Dieser Parameter kann mit allen anderen hier beschriebenen Parametern kombiniert werden.

```
ASignClient_v1.3.2.74_Setup.exe /CRS=YES
```

5 Installation für Windows-Domain Login mit Signaturkarte

Für die Verwendung des a.sign Clients zum Windows-Domain Login ist keine zusätzliche Einstellung mehr notwendig. Bitte beachten Sie auch den Hinweis zur Installation des Microsoft CSP. Kapitel 9.1

6 Vorkonfigurieren der Kartenleser

In der aktuellen Version der Installation werden alle Kartenleser (mit oder ohne Tastaturfeld) verwendet die über eine PCSC Schnittstelle verfügen. Alternativ können die Kartenleser Einstellungen auch nach der Installation über die Registry geändert werden.

Für die Konfiguration der Kartenleser empfiehlt sich folgender Vorgang:

6.1 Kartenleser-Konfiguration vorbereiten

Auf einem Testarbeitsplatz mit installierten a.sign Client kann über die Administrativen Funktionen die gewünschte Kartenleser-Konfiguration hergestellt werden.

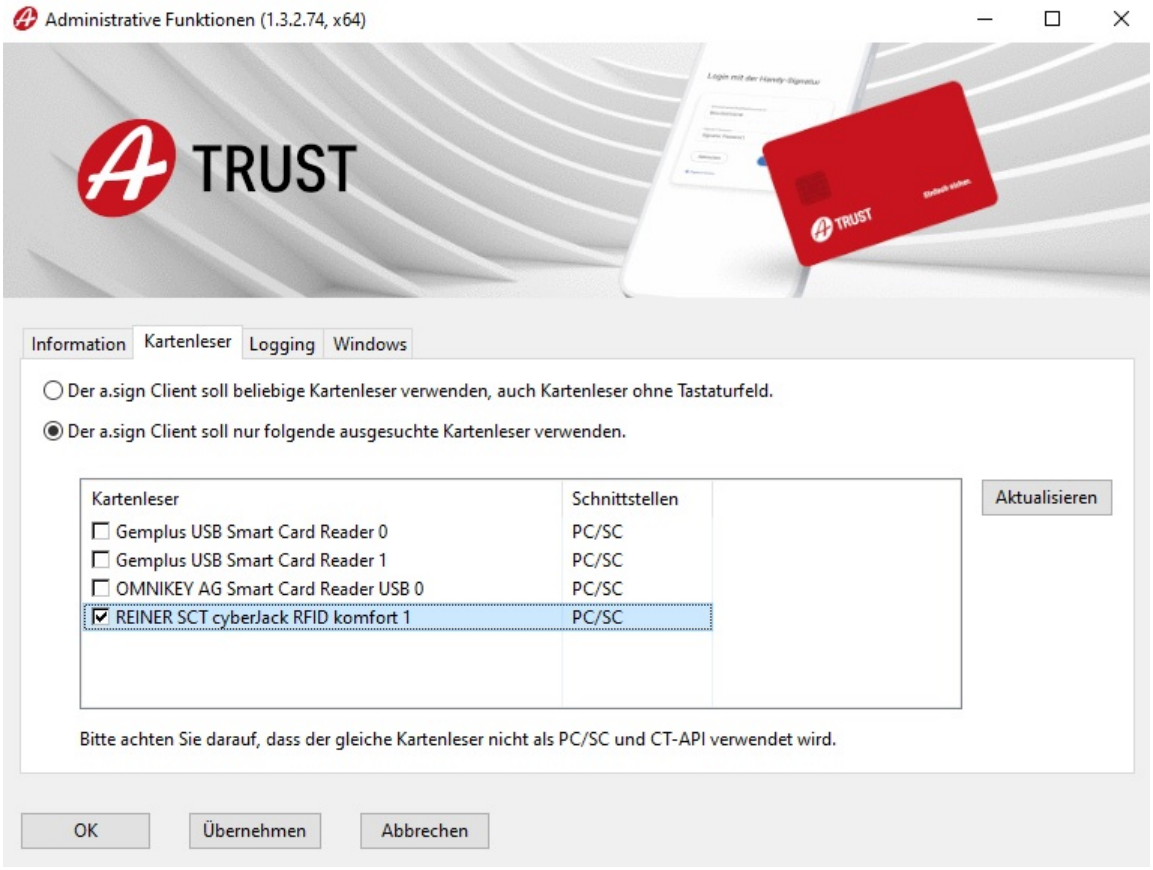

Abbildung 8: Kartenleser

6.2 Einstellungen exportieren

Über den Registry Editor (`regedit.exe`) muss der Registry Zweig

```
HKEY_LOCAL_MACHINE\Software\A-Trust GmbH\a.sign Client
```

als REG-Datei exportiert werden. Falls Sie eine 64bit Umgebung haben müssen Sie auch den Zweig

```
HKEY_LOCAL_MACHINE\Software\Wow6432Node\A-Trust GmbH\a.sign Client
```

exportieren.

6.3 Zusammenfassten von Einträgen

Sie können in der REG-Datei ähnliche Einträge für PCSC-Leser mittels Wildcard („*“) zusammenfassen. Zum Beispiel können Einträge für den REINER SCT CyberJack folgendermaßen zusammengefasst werden:

Original Einträge aus der REG-Datei

```
ReaderName = "REINER SCT cyberJack pinpad/e-com USB 52"
ReaderName = "REINER SCT cyberJack pinpad/e-com USB 53"
ReaderName = "REINER SCT cyberJack pinpad/e-com USB 55"
```

Zusammengefasste Einträge

```
ReaderName = "REINER SCT cyberJack pinpad/e-com USB *"
```

Diese Vorgangsweise umgeht das Problem, dass die Nummerierungen am Ende der PCSC-Readernames oft auf verschiedenen Arbeitsplätzen differieren.

6.4 Installieren der REG-Dateien auf den Zielsystem

Auf den Zielsystemen muss die modifizierte REG-Datei nach der Installation nur noch eingespielt werden.

7 Installationsparameter

7.1 Silent /S

Für die automatische Ausrollung in administrierten Umgebungen ist es hilfreich das Setup ohne Benutzerinteraktion auszuführen, dafür gibt es den Parameter /S.

7.2 Installationsverzeichnis /D=

Ist es gewünscht den a.sign Client in ein spezielles Verzeichnis zu installieren können Sie dieses mit dem Parameter /D=c:\path angeben. Hierbei ist folgendes zu beachten:

- Der Parameter /D muss der letzte Parameter des Aufrufes sein
- Die Pfadangabe darf keine doppelten Anführungszeichen enthalten, auch wenn der Pfad Leerzeichen enthält!

z.B.:

```
ASignClient_v1.3.2.74_Setup.exe /S /D=c:\Programme\A-Trust GmbH\a.sign Client\
```

7.3 Deaktivieren des CRC Check /NCRC

Mit dieser Option wird die Prüfsummenberechnung des Installationsprogrammes deaktiviert.

7.4 CRS Installation /CRS=YES

Für die Installation mit der A-Trust Registrierungssoftware (CRS) wird der Parameter /CRS=YES benötigt.

```
ASignClient_v1.3.2.74_Setup.exe /S /CRS=YES
```

7.5 Automatische Updates /UPDATEABLE=NO

Mit diesem Parameter kann das automatische Update deaktiviert werden.

7.6 Kartenlesereinstellungen behalten /KeepReaders

Mit diesem Parameter werden beim Setup die alten Kartenlesereinstellungen behalten.

```
ASignClient_v1.3.2.74_Setup.exe /KeepReaders /S
```

7.7 A-Trust Reparatur Programm deaktivieren /FixIt=NO

Mit diesem Parameter kann das Reparatur Progamm von A-Trust deaktiviert werden. Das Programm überprüft beim Starten des a.sign Clients, dass die benötigten Dateien vorhanden sind, und installiert diese gegebenenfalls. Dazu werden Administrator Rechte benötigt.

```
ASignClient_v1.3.2.74_Setup.exe /FixIt=NO
```

8 Registry Einträge

Bei 64Bit Betriebssystemen sind alle Registry Keys des a.sign Clients doppelt vorhanden. Einmal für die 32Bit Variante unter

```
HKEY_LOCAL_MACHINE\Software\A-Trust GmbH\...
HKEY_CURRENT_USER\Software\A-Trust GmbH\...
```

und einmal für die 64Bit Variante unter

```
HKEY_LOCAL_MACHINE\Software\Wow6432Node\A-Trust GmbH\...
HKEY_CURRENT_USER\Software\Wow6432Node\A-Trust GmbH\...
```

8.1 Registry Einträge für Microsoft CSP (MiniTreiber)

Registry Einstellungen für den Microsoft Cryptographic Service Provider

8.1.1 Arbeitsplatz Einstellungen

```
HKEY_LOCAL_MACHINE\SOFTWARE\A-Trust GmbH\ASignMiniDriver
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\A-Trust GmbH\AsignMiniDriver
```

EnableATrustPinDialog (DWORD)
0 ... Windows PIN Dialog verwenden (default)
1 ... A-Trust PIN Dialog verwenden

EnableExternalPin (DWORD)
0 ... PIN Eingabe über Windows Dialog
1 ... PIN Eingabe über externe Tastatur, falls der Kartenleser diese Funktion unterstützt (default)

EnableLogging (DWORD)
Logging Datei schreiben
0 ... deaktiviert
1 ... aktiviert (default)

Version (REG_SZ)
Versionsnummer des installierten a.sign Clients

PinCachePolicyType (DWORD)
siehe Kaptiel 8.4
0 ... PinCacheNormal (default)
1 ... PinCacheTimed

2 ... PinCacheNone
3 ... PinCacheAlwaysPromt

PinCachePolicyInfo (DWORD)
siehe Kapitel 8.4

IgnoreAcosSubVersion (DWORD)
Unterscheidung zwischen ACOS03 und ACOS04 Karten...
0 ... deaktiviert
1 ... aktiviert (default)

CheckReaderCapabilities (DWORD)
Es wird überprüft ob der Kartenleser die externe PIN Eingabe unterstützt
0 ... keine Überprüfung
1 ... Überprüfung (default)

EnableDiagnostics (DWORD)
In Fehlerfällen werden anschließend ertweiterte Diagnose Ausgaben im Logfile gespeichert
0 ... deaktiviert (default)
1 ... aktiviert

DoExclusiveReconnect (DWORD)
Beim ersten Aufruf des MiniTreibers wird die bestehende Verbindung zur Karte, im Modus EXCLUSIVE, neu aufgebaut
0 ... deaktiviert (default)
1 ... aktiviert

MiniDriverVersion (DWORD)
Version des MiniTreibers, mögliche Werte sind 4,5,6,7. Der Unterschied zwischen den Versionen kann der Microsoft Spezifikation zum MiniTreiber entnommen werden.

8.1.2 Benutzer Einstellungen

Keine Einstellungen möglich, alle Einstellungen des CSP MiniTreiber werden für den gesamten Arbeitsplatz vorgenommen

8.2 Registry Enträge für PKCS#11 Schnittstelle

8.2.1 Arbeitsplatz Einstellungen

```
HKEY_LOCAL_MACHINE\SOFTWARE\A-Trust GmbH\a.sign Client
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\A-Trust GmbH\a.sign Client
```

CheckForUpdates (REG_SZ)
Dieser Eintrag wird in aktuellen Versionen ingoriert
~~Yes ... nach neuen Versionen suchen~~
~~No ... kein automatisches Update~~

Updateable (REG_SZ)
Dieser Eintrag wird in aktuellen Versionen ingoriert
~~Yes ... Automatische Updates aktiviert~~
~~No ... Automatische Updates deaktiviert~~

InstallDir (REG_SZ)
Installationsverzeichnis des a.sign Client

Version (REG_SZ)
Version des a.sign Client

CRS (REG_SZ)
Anzeige des Signaturzertifikates für alle Applikationen
Yes ... Signaturzertifikat in allen Applikationen anzeigen
No ... Signaturzertifikat nur für die Applikationen in ShowSigFor anzeigen

TraceLogLevel (DWORD)
Logging Level festelgen
128 ... Logging aktiviert
0 ... keine Ausgabe (default)

TraceLogMode (DWORD)
2 ... Logging sofort schreiben
0 ... Logging erst schreiben wenn der Buffer voll ist (default)

TraceFilename (REG_SZ)
Registry Key wird in aktuellen Versionen ignoriert.

Reader0- Reader1- Reader?
Reader Konfiguration siehe Kapitel 6

ShowSigFor
Für alle EXE-Dateien die als Unterorder angelegt sind, wird beim Aufruf der PKCS#11 Schnittstelle das Signaturzertifikat auch angezeigt.

MaxReaderCount (DWORD)
Anzahl der Kartenleser, welche der a.sign Client verwendet. Standardmäßig werden 5 Kartenleser erkannt, eine Erhöhung dieses Wertes wirkt sich negativ auf die Performance aus.

DisableForegroundThreads (REG_SZ)

PIN-Eingabe Dialoge des a.sign Clients werden regelmäßig in den Vordergrund geschoben, sodass die PIN Eingabe nicht hinter einem anderen Fenster verschwinden kann.
Yes ... deaktiveren des "in den Vordergrund schieben" der Dialoge
No ... aktiveren des "in den Vordergrund schieben" der Dialoge (default)

AllowOldOpensslFallback (REG_SZ)

Bei Decrypt Operationen kann es zu Kompatibilitätsproblemen mit älteren OpenSSL Versionen kommen. Ist dieser Registry Wert gesetzt wird in Fehlerfall versucht die Decrypt Funktion aus einer älteren OpenSSL Version aufzurufen.
YES ... im Decrypt-Fehlerfall wird die ältere OpenSSL Funktion aufgerufen
NO ... die ältere Decrpyt-OpenSSL Funktion wird nicht aufgerufen. (default)

MakeDialogsStayOnTop (REG_SZ)

a.sign Client PIN Dialoge und Fehlermeldungen werden als System-Modal angezeigt.
Achtung diese Einstellung kann zu Problemen mit Kartenleser führen, welche selbst einen System-Modal Dialog anzeigen.
YES ... eingeschalten
NO ... ausgeschalten (default)

CacheCertificates (REG_SZ)

Zertifikate die in einer a.sign Client Session gelesen werden, können gecached werden.
YES ... Cache aktivieren
NO ... Cache deaktivieren (default)

8.2.2 Benutzereinstellungen Einstellungen

Positionen der PIN Eingabe Dialoge des a.sign Clients, falls vom Benutzer verschoben.

8.3 Registry Enträge für Applikationen

```
HKEY_LOCAL_MACHINE\SOFTWARE\A-Trust GmbH\a.sign Client
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\A-Trust GmbH\a.sign Client
```

FixIt (REG_SZ)

Beim Windows start wird überprüft ob die PKCS#11 Datei und der CSP MiniTreiber im Windows Verzeichnis vorhanden ist. Falls nicht wird ein Reperaturprogramm

gestartet.
Yes ... Reperaturprogamm ausführen (default)
No ... Reperaturprogamm nicht ausführen

DeleteLogfilesAfterXDays (DWORD)
Beim Windows start werden alte Logdateien aller A-Trust Produkte gelöscht. Wieviele Tag die Logdateien aufgehoben werden kann über diesen Wert eingestellt werden.

CleanCertsOnRefresh (DWORD)
Beim Karten aktualisieren werden die Zertifikate alle gearde nicht eingelegten Signaturkarten aus dem Windows Speicher entfernt.
0 ... Zertifikate behalten
1 ... Zertifikate entfernen

8.4 Mini Treiber PIN Cache Policy

Cache Modus	Beschreibung
PinCacheNormal	In diesem Modus wird die PIN vom Microsoft Base CSP Pro Prozess und Logon ID gecached
PinCacheTimed	In diesem Modus wird die PIN nur für eine definierten Anzahl von Sekunden gehalten. Dies ist implementiert indem der Zeitpunkt der PIN Eingabe gespeichert wird und bei jeder PIN Abfrage der aktuelle Zeitpunkt gegen den gespeicherten Zeitpunkt geprüft wird. Dadurch kann der PIN länger im Cache gehalten werden, als durch die definierte Zeitspanne angegeben. Jedenfalls wird die PIN verschlüsselt im Speicher gehalten um den nötigen Schutz zu gewährleisten. Die Zeit für welche die PIN gespeichert wird, wird über den Registry Key PinCachePolicyInfo in Sekunden angegeben.
PinCacheNone	In diesem Modus wird die PIN nicht gecached. Dadurch müssen alle kryptographischen Funktionen möglichst zeitnahe nach der PIN Eingabe asugeführt werden, bevor das Transaktionstimeout des Base-CSP abläuft.
PinCacheAlwaysPromt	In diesem Modus wird die PIN nicht gecached, im Unterschied zu PinCacheNone wird vor jeder kryptographischen Funktion die PIN erneut abgefragt.

Tabelle 2: Mini Treiber Pin Cache Policy

Sollte der Cache Modus auf einen anderen Wert als PinCacheNormal gesetzt werden, kann es zu Probleme mit der Windows Anmeldung kommen. Dieses Verhalten ist durch Microsoft so vorgesehen.

Originaltext zum PIN- Caching ist in der Microsoft MiniTreiber Spezifikation enthalten http://msdn.microsoft.com/en-us/library/windows/hardware/gg487500.aspx SC-Minidriver_spec_v7.docx, Kapitel 4.2.1.4

9 Installationshinweis

9.1 Installation Microsoft CSP

Warum kann es auf manchen Computer, Dateien in der Form ASignMiniDriver5.dll, geben?

Wenn auf dem Computer bereits ein a.sign Client installiert ist, kann der A-Trust Mini Treiber (Schnittstelle Microsoft CSP) bereits vom Betriebssystem geladen und blockiert sein. In diesem Fall kann die bereits vorhandene Datei bei einer Installation nicht gelöscht werden.

Dieses Problem wird gelöst indem die aktuelle Version unter einem anderen Namen abgelegt und registriert wird (z.B.: `ASignMiniDriver5.dll`). Somit sind auf dem Computer zwar zwei Mini Treiber Dateien installiert, jedoch wird für alle zukünftigen Zugriff die korrekte Version verwendet.

Bei der nächsten Installation werden alle nicht mehr benötigten Mini Treiber Dateien gelöscht (Rechteproblem).

Diese Betrachtungen werden für 32bit und 64bit getrennt vorgenommen, es kann daher vorkommen, dass auf einem 64bit System eine `ASignMiniDriver.dll` im `system32` Verzeichnis vorhanden ist und eine `ASignMiniDriver2.dll` im `SysWOW64` Verzeichnis.

9.2 USB Kartenleser - Kartenleser wird von Windows abgeschalten

In Windows 7 und 8 wurde eine Power-Saving Funktion für USB Geräte eingeführt. Diese Funktion sendet dem Kartenleser ca. 30 Sekunden nach der letzten Transaktion einen Power-Off Befehl. Dies führt z. B. zum Abmelden durch das Betriebssystem, da die Karte nicht mehr erkannt wird.

Um das Power-Down Kommando an den Kartenleser zu verzögern, kann der nachfolgende Registry Key gesetzt werden:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\calais\
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\calais\
```

CardDisconnectPowerDownDelay (DWORD)
Der Standard Wert für diesen Eintrag ist 30 (Sekunden), eine Erhöhung des Wertes bis auf 3600 (1 Stunde) ist möglich.

9.3 Domain Anmeldeprobleme nach Neustart bei langsamen Verbindungen

Bei langsamen Verbindungen oder erhöhter Reaktionszeit des Domainkontrollers, kann es zu Problemen beim Erkennen des Anmeldeservers durch das lokale Betriebssystem kommen. Abhilfe schafft die Erhöhung des Timeouts beim Erkennen des Anmeldeservers:

`HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\`

ExpectedDialupDelay (DWORD)
(http://technet.microsoft.com/en-us/library/cc957332.aspx)