Infineon Security Platform

Security Platform  Trusted Platform Module

http://www.infineon.com/tpm/software

Infineon Technologies AG
Infineon Security Platform
Infineon Security Platform  Trusted Platform Module
  .  Infineon Trusted Platform Module
  .

- Microsoft Windows Mail/Outlook Express, Microsoft Outlook
  Mozilla Thunderbird
- (: Mozilla Firefox  Internet Explorer) (: Microsoft Internet Information Server).
- Microsoft Word .
- .
- .

Infineon Security Platform .

- Security Platform
- Security Platform
- Security Platform
- Security Platform
- Security Platform
- Security Platform
- Security Platform
- Security Platform
- Security Platform
- Security Platform PKCS #12
- Security Platform
- Security Platform
- Security Platform
- Security Platform
- Security Platform
- Server Integration Services
- Personal Secure Drive

**Infineon Security Platform**
Infineon Trusted Platform Module  Infineon Security Platform

- 
- 
- 

- **Internet Information Server**  **Active Directory**
- **Internet Explorer**,  **Mozilla Firefox**
- **Microsoft Word**

     .  Security Platform

---

Technologies AG
Infineon Security Platform Solution
Trusted Platform Module

- Trusted Platform Module (TPM)
- TCG
- TRNG (True Random Number generator)
- SPA (Simple Power Analysis)
- DPA (Differential Power Analysis)

©Infineon Technologies AG
Infineon Security Platform
Microsoft Windows

Microsoft Windows
Windows Vista.

"Windows 7.

Microsoft BitLocker

Windows Vista edition  Microsoft BitLocker
  . TPM(Trusted Platform Module)  BitLocker
  . TPM(Trusted Platform Module)

  _______  Infineon Security Platform  .
TPM ( )

Microsoft TPM (Trusted Platform Module) Windows Vista
. Trusted Platform Module .
Microsoft TechNet . Microsoft TechNet .
Windows Vista   TPM  TSS  TPM
Windows   .

Technologies AG
Infineon Security Platform -
Server Integration Services  Security Platform Trust Domain.

*Trusted Computing Management Server*

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Trust Domain (Trusted Computing Management Server).
- Trusted Platform Module.
- Trusted Platform Module (Infineon TPM Trusted Domain, Windows Trusted Platform Module(TPM)).
- Trust Domain., Trust Domain.

- Trust Domain (Trusted Computing Management Server).
- Trusted Platform Module.
- Trust Domain., Trust Domain.
Security Platform   Trust Domain .
<table>
<thead>
<tr>
<th></th>
<th>Security Platform</th>
<th>Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security Platform</td>
<td>Trusted Computing</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td>Management Server</td>
</tr>
<tr>
<td></td>
<td>( )</td>
<td>Trust Computing Management Server</td>
</tr>
<tr>
<td></td>
<td>Security Platform , ( )</td>
<td>Trust Domain ,</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td>Security Platform</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td>Trusted Computing Management Server</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td>, ,</td>
</tr>
<tr>
<td></td>
<td>, Personal Secure Drive(PSD)</td>
<td>Server Integration Services , Personal Secure Drive(PSD)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trusted Computing Management Server</td>
</tr>
<tr>
<td>PKCS #12</td>
<td>Personal Information Exchange Security Platform</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Infineon Security Platform
Infineon Security Platform

1. Infineon Security Platform,

2. InstallShield Infineon Security Platform

3. .

4. EULA .

5. .

6. .

7. .
   • .
   • .

8. .
   Infineon Security Platform .

9. .

10. .


   • Security Platform
   • Security Platform
   • Security Platform
- Security Platform
- Security Platform
- Security Platform
- Security Platform
- Security Platform PKCS #12
- Security Platform
- Security Platform
- Personal Secure Drive
- Infineon TPM Cryptographic Service Providers
- Security Platform
- Trusted Platform Module
- Server Integration Services

12. Infineon Security Platform


14. **readme**

15. 

Infineon Technologies AG
Infineon Security Platform
Infineon Security Platform

- Infineon Security Platform
- Trust Domain
- Security Platform

Infineon Security Platform

- Infineon Security Platform

Infineon Security Platform

Security Platform

(FAQ)

©Infineon Technologies AG
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Platform</td>
<td>Windows ( )</td>
<td>Windows ( )</td>
<td>Windows ( )</td>
</tr>
</tbody>
</table>

...
<table>
<thead>
<tr>
<th>EFS/PSD</th>
<th>EFS/PSD</th>
<th>EFS/PSD</th>
</tr>
</thead>
<tbody>
<tr>
<td>(&quot;&quot;)</td>
<td>EFS</td>
<td>EFS</td>
</tr>
<tr>
<td></td>
<td>PSD</td>
<td>PSD</td>
</tr>
</tbody>
</table>

Infineon  Technologies AG
Infineon Security Platform
Infineon Security Platform . ,
. Security
Platform .

Infineon Security Platform
.


. , USB ,
. PIN
.
PIN

(Brute-Force)

PIN

Security Platform

•

•
. Security Platform
.
., Security Platform
.
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **2.** | Security Platform : ...
|   | Security Platform : ___
|   | - - ___
| **3.** | Security Platform : ___
|   | - - ___

Infineon Technologies AG
Infineon Security Platform
<table>
<thead>
<tr>
<th>Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infineon Security Platform</td>
</tr>
<tr>
<td>(: ). Security Platform</td>
</tr>
<tr>
<td>Security Platform</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>/</th>
</tr>
</thead>
<tbody>
<tr>
<td>( ).</td>
<td>Microsoft &quot;Trusted Platform Module(TPM) Management&quot;</td>
</tr>
<tr>
<td></td>
<td>Trusted Computing Management Server</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Platform , Security Platform</td>
<td></td>
</tr>
<tr>
<td>Personal Secure Drive .</td>
<td></td>
</tr>
<tr>
<td>Trusted Platform Module .</td>
<td></td>
</tr>
</tbody>
</table>

| Security Platform | ( Security Platform | Security Platform | (trusted Platform Module ) |
| Security Platform | Trusted Computing Management Server |

```
<table>
<thead>
<tr>
<th>Platform</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>_ _ Trusted Platform</td>
<td></td>
</tr>
<tr>
<td>Computing Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>/</td>
<td>Security Platform ( Security Platform )</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>_ _ Trusted Computing Management Server</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>/</td>
<td></td>
</tr>
<tr>
<td></td>
<td>_ _ Trusted Computing Management Server</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>PKCS #12 ( )</td>
<td></td>
</tr>
</tbody>
</table>
Infineon Security Platform
Security Platform

Security Platform

EFS PSD

Infineon Technologies AG
Infineon Security Platform
Security Platform

<table>
<thead>
<tr>
<th>Security Platform . Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>Security Platform .</td>
</tr>
<tr>
<td>Personal Secure Drive . Security Platform</td>
</tr>
<tr>
<td>(: ) Security Platform .</td>
</tr>
</tbody>
</table>

- Personal Secure Drive(PSD)
- Trusted Computing Management Server .
- Trusted Computing Management Server .
## Security Platform

<table>
<thead>
<tr>
<th>Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Platform</td>
</tr>
</tbody>
</table>

- Security Platform
- Security Platform
- Security Platform
- Security Platform

- "", : SPSytemBackup.xml


- ( Security

- Platform ). ID

- ID


- Security Platform ( Security

- Platform ). ID

- ID

## Trusted Platform Module

<table>
<thead>
<tr>
<th>Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Platform</td>
</tr>
</tbody>
</table>

- Security Platform

- Security Platform

- Security Platform

- Security Platform

- Security Platform

## Personal Secure Drive

<table>
<thead>
<tr>
<th>Personal Secure Drive</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSD, .</td>
</tr>
</tbody>
</table>
PSD

:  
  - PSD
  - PSD PSD

Personal Secure Drive

- PSD
- **PSD** (: SpPSDBackup.fsb): Security Platform
  PSD
<table>
<thead>
<tr>
<th>Personal Secure Drive(PSD)</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security Platform, Personal Secure Drive</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Trusted Platform Module</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Platform</td>
<td>Security Platform, Personal Secure Drive</td>
<td></td>
</tr>
</tbody>
</table>
Security Platform:

- Infineon Security Platform Settings Tool.

- Security Platform
  - ( )
  - XML (: SPSysSystemBackup.xml) (: SPSysSystemBackup)
    - \%ALLUSERSPROFILE\My Documents\Security Platform.
      - 12:00.
        ...
  - ( : SPEmRecToken.xml)
    - ...
Security Platform

Security Platform:
- Infineon Security Platform Settings Tool
- ...
- ...
- XML (:SPSystemBackup.xml (:SPSystemBackup)
- \%ALLUSERSPROFILE\My Documents\Security Platform.
- 12:00 .
- ...
- ...
- " "
- ...
- Security Platform
- ...

Trusted Computing Management Server

(" ")

: ...
: ...
: ...
: Infineon Security Platform Settings Tool ...
• ... .
• ...
  ( : SpBackupArchive.xml).
• Personal Secure Drive
  ( Personal Secure Drive
    )
• .
• .

\[ \text{Personal Secure Drives (PSD) .}
\text{Trusted Computing Management Server}
\]
.  PSD(Personal Secure Drive)
.

\[ \text{Infineon Security Platform}
\text{Settings Tool .}
\]
\[ \text{Security Module - -...}
\]
• .
• .

\[ \text{... ( : SPBackupArchive.xml) .} \]
- Personal Secure Drive
- Security Platform
- Trusted Computing Management Server
* Security Platform

Infineon Technologies AG
Infineon Security Platform
Infineon Security Platform

Trusted Platform Module

Infineon Security Platform

Trusted Platform Module

Infineon Security Platform

Trusted Platform Module

Infineon Security Platform (PSD)

PSD (Personal Secure Drive)

Trusted Computing Management Server
Trusted Platform Module
Security Platform
Security Platform
Security Platform

(FAQ)

: ( ; Trusted Platform Module
 ) Security Platform

: ( )

: Security Platform

: SpUserWz.exe /forceinit.

: SpUserWz.exe /forceinit
Infineon Security Platform
Trusted Platform Module    Infineon Security Platform

Security Platform:


Trust Domain  Trusted Platform Module
- Trusted Computing Management Server

Security Platform:

- 

FAQ

- PSD(Personal Secure Drive)
- Trusted Computing Management Server
<table>
<thead>
<tr>
<th><strong>1 - Trusted Platform Module</strong></th>
<th>:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Platform Module</td>
<td></td>
</tr>
<tr>
<td>BIOS</td>
<td></td>
</tr>
<tr>
<td>( :</td>
<td></td>
</tr>
<tr>
<td>) (</td>
<td></td>
</tr>
<tr>
<td>) Infineon Security Platform</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>2 - Security Platform</strong></td>
<td>:</td>
</tr>
<tr>
<td>Trusted Platform Module</td>
<td></td>
</tr>
<tr>
<td>Security Platform</td>
<td></td>
</tr>
<tr>
<td>Infineon Security Platform</td>
<td></td>
</tr>
<tr>
<td>Security Platform</td>
<td></td>
</tr>
<tr>
<td>Infineon Security Platform</td>
<td>:</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---</td>
</tr>
<tr>
<td>Infineon Security Platform</td>
<td>Security Platform</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>Infineon</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>,</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
</tbody>
</table>
Infineon Security Platform
Windows

- ( ) Trusted Computing Management Server ( ).
- (: ).
- (: ).
- (: ).

- Personal Secure Drive .
Infineon Security Platform
EFS PSD

EFS PSD :

- 
- 
- (EFS, PSD ).
- .

Microsoft TechNet .

PSD Personal Secure Drive .

©Infineon Technologies AG
Infineon Security Platform
Infineon Security Platform
Infineon Security Platform

Infineon Security Platform

Trusted Platform Module

Infineon Security Platform

Trusted Computing Management Server

Infineon Security Platform

Security Platform

( ): Security Platform

( ): EFS PSD

Personal Secure Drive:
- Personal Secure Drive (: USB )
- Personal Secure Drive

Personal Secure Drive
Personal Secure Drive

Personal Secure Drive

Personal Secure Drive (Personal Secure Drive)

- PSD

PSD (Personal Secure)
Infineon Security Platform
Trusted Computing Management Server

(34)
Infineon Security Platform

- Infineon Security Platform Module
- 

SpPubKeyArchive.xml

() Infineon Security Platform

- Infineon Security Platform Settings Tool
- 
- ... 
- 

SpPubKeyArchive.xml
<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Infineon Security Platform</strong></td>
<td></td>
</tr>
<tr>
<td>Infineon Security Platform DCOM</td>
<td></td>
</tr>
<tr>
<td>Infineon (</td>
<td></td>
</tr>
<tr>
<td>)</td>
<td>(</td>
</tr>
<tr>
<td>)</td>
<td></td>
</tr>
<tr>
<td>:</td>
<td></td>
</tr>
<tr>
<td>• : Infineon Security Platform</td>
<td></td>
</tr>
<tr>
<td>• : SRK</td>
<td></td>
</tr>
<tr>
<td>• : DCOM</td>
<td></td>
</tr>
<tr>
<td>(Infineon Security Platform</td>
<td></td>
</tr>
<tr>
<td>)</td>
<td></td>
</tr>
<tr>
<td>• : DCOM (: Microsoft Windows XP</td>
<td></td>
</tr>
<tr>
<td>)</td>
<td></td>
</tr>
<tr>
<td>DCOM</td>
<td></td>
</tr>
<tr>
<td>(1 2)</td>
<td></td>
</tr>
<tr>
<td>1 -</td>
<td>:</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>&quot;&quot;&quot; .</td>
<td>• Infineon Security Platform Settings Tool .</td>
</tr>
<tr>
<td>.</td>
<td>• .</td>
</tr>
<tr>
<td>.</td>
<td>• .</td>
</tr>
<tr>
<td>.</td>
<td>• .</td>
</tr>
<tr>
<td>.</td>
<td>• .</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>SpMigrationArchive.xml</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>2 -</td>
<td>:</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
</tbody>
</table>
- Infineon Security Platform Settings Tool

- ...

- SpMigrationArchive.xml

- ...

- Security Platform

- ...

- Security Platform

- ! Personal Secure Drive

3 -
<table>
<thead>
<tr>
<th>4 - Personal Secure Drive</th>
<th>:</th>
</tr>
</thead>
</table>

Infineon Technologies AG
Infineon Security Platform
Security Platform

- Trusted Computing Management Server
Security Platform
Security Platform
Security Platform
Security Platform
Security Platform
Security Platform:

- Infineon Security Platform Settings Tool.
- (SPPwdResetToken.xml)

- (SPPwdResetSecret.xml)
- Security Platform
- ...
- Infineon Security Platform Settings Tool
- ...
- (SPPwdResetSecret.xml)
3. : 

- - ... __________ ( ) 

: 

- Infineon Security Platform Settings Tool .
- ... .
- .
- ( : SPPwdResetToken.xml )
  .
  .
  ( : SPPwdResetCode.xml ) (: ) . .

- Infineon Security Platform Settings Tool .
- ... .
- .
- ( : SPPwdResetToken.xml )
  .
  .
  ( : SPPwdResetSecret.xml )
  .
  .
  .
  .
Infineon Security Platform

Settings Tool

SPPwdResetSecret.xml

SPPwdResetCode.xml
Infineon Security Platform
- Trusted Platform Module 1.2 Security Platform.
  Infineon Trusted Platform Module 1.2 Security Platform.
- Security Platform.
Security Platform :

- Microsoft

Security Platform

Technologies AG
Infineon Security Platform
Trusted Platform Module 1.2 Security Platform.

- Security Platform
- Infineon Trusted Platform Module 1.2 Security Platform.
- Security Platform.

Security Platform:
- Security Platform
- Security Platform
- Security Platform.
- Security Platform.
Security Platform
Security Platform

Security Platform.

Security Platform.

Security Platform.
T Security Platform.

, ( ) ( )

. Security Platform

.
<table>
<thead>
<tr>
<th>Description</th>
<th>Value 1</th>
<th>Value 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Security Platform)</td>
<td>5</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>6 5</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>(_____</td>
<td>_____</td>
</tr>
<tr>
<td></td>
<td>_______)</td>
<td></td>
</tr>
<tr>
<td>Security Platform</td>
<td>3</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>6 3</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>(_____</td>
<td>_____</td>
</tr>
<tr>
<td></td>
<td>_______)</td>
<td></td>
</tr>
<tr>
<td>(: PIN Windows BitLocker :)</td>
<td>10</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>6 10</td>
<td>-</td>
</tr>
</tbody>
</table>
|                                    | (_____  | _______)
|                                    | _______|        |
|                                    | ~10 s   | 10.     |
|                                    | ~24 h   | 24.     |
|                                    | ~6 h    | 6       |
|                                    | 6 1.    | 6       |
|                                    | 1.      | 1.      |

©Infineon Technologies AG
Infineon Security Platform
- Trusted Platform Module 1.2 Security Platform.
- Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.
Security Platform

(Security Platform)

( )
- Trusted Platform Module 1.2 Security Platform
  - Security Platform
  - Infineon Trusted Platform Module 1.2 Security Platform.
  - Security Platform.

- Security Platform
  - Trusted Computing Group (TCG) Trusted Platform Module
  - Security Platform.

- Security Platform
  - Trusted Platform Module
  - Security Platform.

- Security Platform
  - Trusted Platform Module
  - Security Platform.

- Security Platform
  - Trusted Platform Module
  - Security Platform.
<table>
<thead>
<tr>
<th></th>
<th>Security Platform</th>
</tr>
</thead>
</table>

©Infineon Technologies AG
- Trusted Platform Module 1.2 Security Platform.
- Security Platform
- Infineon Trusted Platform Module 1.2 Security Platform.
- Security Platform
1. Security Platform
   - PIN
   - Windows BitLocker
   - Trusted Platform Module

   ("F5")

2. Security Platform

   Trusted Platform Module
Infineon Security Platform

<table>
<thead>
<tr>
<th>Security Platform</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Platform</td>
<td>• Trusted Platform Module .</td>
</tr>
<tr>
<td>Security Platform</td>
<td>• .</td>
</tr>
<tr>
<td>Security Platform</td>
<td>• Infineon Security Platform ( ).</td>
</tr>
<tr>
<td>Security Platform</td>
<td>• Infineon Security Platform ( ).</td>
</tr>
<tr>
<td>Security Platform</td>
<td>• Infineon Security Platform ( ).</td>
</tr>
<tr>
<td>Security Platform</td>
<td>• Infineon Security Platform ( ).</td>
</tr>
<tr>
<td>Security Platform</td>
<td>• Security Platform .</td>
</tr>
<tr>
<td>Security Platform</td>
<td>• .</td>
</tr>
<tr>
<td>Security Platform</td>
<td>• Security Platform .</td>
</tr>
<tr>
<td>Security Platform</td>
<td>• Security Platform .</td>
</tr>
<tr>
<td>Security Platform</td>
<td>• Infineon Security Platform</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Security Platform</td>
<td>• Trusted Platform Module</td>
</tr>
<tr>
<td>Security Platform</td>
<td>• Trusted Computing Group (TCG)</td>
</tr>
</tbody>
</table>

Technologies AG
Infineon Security Platform
Security Platform

Security Platform   Infineon Security Platform
Security Platform

: Security Platform (Platform )
( ).

Security Platform
Security Platform . .
| --- | --- |
|   | Windows
|   | Trusted Platform Module |
| Security Platform | Security Platform |
| Security Platform | , PKCS #12 :
|   | Security Platform |
| Security Platform /Security Platform ( ):
|   | Security Platform
|   | Infineon Security Platform |
|   | Trusted Platform Module
|   | Infineon Security Platform |
|   | Trusted Platform Module
|   | Trusted Platform Module |
| Trusted Platform Module | Infineon Security Platform |
|   | Security Platform |
|   | . |
Infineon Security Platform

•
•

Security Platform

- Security Platform
- Security Platform
- ________
<table>
<thead>
<tr>
<th>Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN (</td>
</tr>
<tr>
<td>.</td>
</tr>
<tr>
<td>).</td>
</tr>
</tbody>
</table>
## Security Platform

<table>
<thead>
<tr>
<th>Security Platform</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Platform</td>
<td></td>
</tr>
<tr>
<td>Security Platform</td>
<td></td>
</tr>
<tr>
<td>Security Platform</td>
<td></td>
</tr>
<tr>
<td>USB</td>
<td></td>
</tr>
<tr>
<td>PIN</td>
<td>USB PIN</td>
</tr>
<tr>
<td>Security Platform</td>
<td></td>
</tr>
<tr>
<td>Security Platform</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>☑</td>
<td>Security Platform</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Security Platform

<table>
<thead>
<tr>
<th>Security Platform</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(, )</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>USB</th>
<th>PIN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>(: )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>USB</th>
<th>PIN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>USB</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>PIN</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
</tbody>
</table>

|     | (: ) |
| ( , ) |     |

|     |
|     | .    |

|     |
|     | .    |

<table>
<thead>
<tr>
<th>USB</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Infineon Technologies AG
Infineon Security Platform
Security Platform


<table>
<thead>
<tr>
<th></th>
<th></th>
<th>/</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>( )</td>
<td>Microsoft &quot;Trusted Platform Module (TPM) Management&quot;</td>
</tr>
<tr>
<td></td>
<td>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>.</td>
<td>&quot;&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;&quot;</td>
<td>.</td>
</tr>
</tbody>
</table>
|                | Security Platform . | ""

Trusted Computing Management Server
<table>
<thead>
<tr>
<th>PKCS #12</th>
<th>PKCS #12</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• ., Windows . Security Platform
  Windows . Windows
  EFS PSD
  Security Platform .
• .
  .
• .
• .
• .
• .
- (A-Z)
- (a-z)
- 10 (0-9)
- (!:!, $, #, %)
Infineon Security Platform

Infineon Technologies AG
Infineon Security Platform -
## Infineon Security Platform

Security Platform  Trusted Platform Module

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Infineon Security Platform

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- ()
- (

- Trusted Computing Management Server
- PSD(Personal Secure Drive)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Security Platform
- Security Platform

- Trusted Computing Management Server

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- BitLocker

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Trusted Platform Module  BitLocker
- BitLocker (Windows 7, Windows Vista Enterprise, Ultimate editions).
- Microsoft BitLocker BitLocker.

- Security Platform
- Security Platform /
- Security Platform

- Trusted Computing Management Server
  Security Platform.
• Security Platform
  (: Windows 7  Windows Vista)
  
• Security Platform
  (: Windows 7  Windows Vista)

Infineon Technologies AG
## Infineon Security Platform

<table>
<thead>
<tr>
<th>Infineon Security Platform</th>
<th>Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Platform Module</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>Infineon Security Platform</td>
<td></td>
</tr>
</tbody>
</table>
Infineon Security Platform -
| Security Platform | (*.txt) |

Infineon Technologies AG
Infineon Security Platform -
Security Platform

Infineon Security Platform :
(Trusted Platform Module )

Trusted Platform Module .

- Infineon Security Platform Trusted Platform Module

- Trusted Platform Module . BIOS
Infineon Security Platform .
  Trusted Platform Module BIOS BIOS .
  Infineon Security Platform Trusted Platform Module

- Trusted Platform Module .
Infineon Security Platform.

- Infineon Security Platform


- Infineon Security Platform
  Infineon Security Platform Security Platform
  (1):
  Security Platform

TPM, Security Platform - Infineon Security Platform
"OS".

1: Windows 7 Windows Vista Microsoft TPM(____)

Trusted Platform Module ., Trusted Platform Module Infineon Security Platform

2: ,

Infineon Security Platform Security Platform
(2):
Security Platform
- Infineon Security Platform

(: )

Security Platform Security Platform

- Infineon Security Platform

( ).


(:

Security Platform Security Platform

).
Trusted Computing Management Server

Infineon Technologies AG
Infineon Security Platform -
Infineon Security Platform

- Security Platform
- Infineon Security Platform
  - Trust Domain
- Security Platform
  -

- Infineon Security Platform
  -

<table>
<thead>
<tr>
<th>Security Platform / / .</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infineon Security Platform</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Infineon Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Infineon Technologies AG
Infineon Security Platform -
Infineon Security Platform


- Security Platform
  - Trusted Computing Management Server

<table>
<thead>
<tr>
<th></th>
<th>Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Infineon Security Platform</td>
</tr>
</tbody>
</table>

- Personal Secure Drive
  - PSD

<table>
<thead>
<tr>
<th></th>
<th>Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Infineon Security Platform</td>
</tr>
</tbody>
</table>

- Trusted Computing Management Server
<table>
<thead>
<tr>
<th>Infineon Security Platform</th>
<th>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>. PSD(Personal Secure Drive)</td>
<td>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Platform</th>
<th>. Personal Secure Drive (PSD)</th>
</tr>
</thead>
</table>

| . | . |

| . | . |
Infineon Security Platform -
Infineon Security Platform

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Image" /></td>
<td>Security Platform</td>
</tr>
<tr>
<td><img src="image2.png" alt="Image" /></td>
<td>Trusted Computing Management Server</td>
</tr>
</tbody>
</table>

| ![Image](image3.png) | Infineon Security Platform |
| ![Image](image4.png) | Infineon Security Platform |
| ![Image](image5.png) | Infineon Security Platform |

| ![Image](image6.png) | Infineon Security Platform |
| ![Image](image7.png) | Security Platform |
| ![Image](image8.png) | Infineon Security Platform |
| ![Image](image9.png) | Infineon Security Platform |

| ![Image](image10.png) | Infineon Security Platform |
| ![Image](image11.png) | Security Platform |
| ![Image](image12.png) | Infineon Security Platform |
| ![Image](image13.png) | Infineon Security Platform |
| Security Platform
| --- |
| Infineon Security Platform
| Infineon Security Platform |
| Infineon Security Platform |
| Infineon Security Platform |

Infineon Technologies AG
Infineon Security Platform -
Infineon Security Platform

-  __ Security Platform __
-  __ Trusted Computing Management Server __
Infineon Security Platform -
BitLocker

TPM (Trusted Platform Module) BitLocker
. BitLocker Microsoft BitLocker .

- BitLocker (: Windows 7 Windows Vista
  Enterprise Ultimate editions) .
- ~ .

BitLocker .

<table>
<thead>
<tr>
<th>abc</th>
<th>BitLocker .: , , , , .</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;</td>
<td>Microsoft BitLocker .</td>
</tr>
<tr>
<td>&quot;</td>
<td>TPM(Trusted Platform Module)</td>
</tr>
</tbody>
</table>

Technologies AG
Infineon Security Platform -
Infineon Security Platform

- Security Platform
- Infineon Security Platform
- Windows editions (Windows Home editions)
- Security Platform

<table>
<thead>
<tr>
<th>Security Platform</th>
<th>Infineon Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Domain</td>
<td>Security Platform</td>
</tr>
<tr>
<td></td>
<td>Infineon Security Platform</td>
</tr>
<tr>
<td></td>
<td>Trusted Computing Management Server</td>
</tr>
</tbody>
</table>

Infineon Security Platform
- Infineon Trusted Platform Module 1.2 Security Platform

Security Platform:

- EFS, Personal Secure Drive
- Trusted Platform Module
- Security Platform
- Security Platform

BitLocker (Windows Vista Enterprise Ultimate) Security Platform

BIOS Security Platform:

- BIOS
- Security Platform
- BIOS Security Platform (Trusted Platform Module).

- BIOS Infineon Security Platform
- Infineon Security Platform
- \[\text{resetattack}\]

Security Platform:

- SpTPMWz.exe
- Trusted Platform Module 1.2 Security Platform
- Trusted Platform Module
<table>
<thead>
<tr>
<th></th>
<th>Windows editions:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Windows Home editions</td>
</tr>
<tr>
<td></td>
<td>- Trusted Computing Management Server</td>
</tr>
</tbody>
</table>

- Infineon Security Platform

- Windows Home editions
- Trusted Computing Management Server
Infineon Security Platform -
Trusted Computing Management Server
Infineon Security Platform -
Infineon Security Platform

- Security Platform
- Management provider

- Trust Domain Security Platform
<table>
<thead>
<tr>
<th></th>
<th>Trusted Platform: (Platform Module).</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Security Platform: (EFS), Personal Secure Drive (PSD), (Security Platform).</td>
</tr>
<tr>
<td>3.</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>, ,</td>
</tr>
<tr>
<td>6.</td>
<td>,</td>
</tr>
</tbody>
</table>
Security Platform : 

Security Platform : EFS PSD 

©Infineon Technologies AG
Infineon Security Platform -
Security Platform

BitLocker (USBD)

Personal Secure Drive (PSD)

©Infineon Technologies AG
Infineon Security Platform -
Security Platform

: 

- Management provider
- EFS Windows Home editions
- EFS
- PSD

Security Platform

<table>
<thead>
<tr>
<th>(EFS)</th>
<th>EFS Microsoft NTFS . EFS  Security Platform Solution Trusted Platform Module EFS . EFS , Documents\Encrypted Data My Documents\Encrypted Data ( ), . EFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Secure Drive (PSD)</td>
<td>PSD . PSD  PSD  PSD  PSD . PSD . PSD ( )  Personal Secure Drive Security Platform</td>
</tr>
<tr>
<td></td>
<td>Security Platform .</td>
</tr>
</tbody>
</table>
### EFS PSD?

**EFS PSD , .

<table>
<thead>
<tr>
<th>EFS</th>
<th>PSD</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>' </code>'</td>
<td><code>' '</code></td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>Windows Home editions</td>
<td>Security Platform Solution</td>
</tr>
<tr>
<td>Security Platform Solution</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>( )</td>
</tr>
<tr>
<td>. EFS</td>
<td>. PSD</td>
</tr>
<tr>
<td>. , NTFS</td>
<td>. , NTFS</td>
</tr>
<tr>
<td>EFS .</td>
<td>EFS : EFS</td>
</tr>
<tr>
<td></td>
<td>EFS : PSD</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>, NTFS</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>Security Platform Solution</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td><strong>EFS PSD</strong></td>
<td>(** My Documents**)</td>
</tr>
<tr>
<td></td>
<td>Windows Home edition EFS</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>Personal Secure Drive</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Infineon Technologies AG
Infineon Security Platform -
Infineon Security Platform -
USB ) . . , (: .
TPM

Technologies AG
Infineon Security Platform
<table>
<thead>
<tr>
<th>![Image]</th>
<th>![Image]</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>![Image]</td>
<td>![Image]</td>
</tr>
</tbody>
</table>

© Infineon Technologies AG
Infineon Security Platform -
<table>
<thead>
<tr>
<th>(USB, HD)</th>
<th>Security Platform</th>
<th>(USB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>: SpOwner_&lt;PC&gt;_.tpm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;PC&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(: USB )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>. USB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(: USB ).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>/ (HD)</th>
<th></th>
<th>/ (USB, HD)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>: SpToken_&lt;PC&gt;_.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;PC&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(: USB )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(USB, HD)</th>
<th></th>
<th>(USB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>: SpPwdResetSecret_&lt;PC&gt;_User.xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;PC&gt; , &lt;User&gt;</td>
</tr>
</tbody>
</table>
Infineon Security Platform -
Infineon Security Platform

Infineon Security Platform (, , , BitLocker).
Infineon Security Platform

: 

• 

• ( .)


Trust Domain Security Platform .


<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.</strong> Trusted Platform Module</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td><strong>2.</strong> ?___________</td>
<td>Security Platform</td>
</tr>
<tr>
<td><strong>3.</strong> __ __</td>
<td>Security Platform</td>
</tr>
<tr>
<td><strong>4.</strong> .</td>
<td>.</td>
</tr>
<tr>
<td><strong>5.</strong> .</td>
<td>.</td>
</tr>
<tr>
<td><strong>6.</strong> __</td>
<td>.</td>
</tr>
<tr>
<td><strong>7.</strong> __</td>
<td>.</td>
</tr>
<tr>
<td><strong>8.</strong> BitLocker</td>
<td><em>BitLocker</em></td>
</tr>
<tr>
<td></td>
<td>BitLocker</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td><strong>9.</strong> __</td>
<td>Security Platform</td>
</tr>
<tr>
<td><strong>10.</strong> ____________</td>
<td>Infineon Trusted Platform Module 1.2 Security Platform</td>
</tr>
</tbody>
</table>
Security Platform :  Security
Platform .  . Security
Platform .

Security Platform : Security Platform
.
  • Security Platform ( , , ):  
    - - 
  • :  
  • :  

Infineon Technologies AG
Infineon Security Platform -
Trusted Platform Module

TPM (Trusted Platform Module) . Security Platform . Trusted Platform Module

**Physical Presence Interface (PPI)**

**Trusted Platform Module 1.2**

Trusted Platform Module . BIOS

.:  

<table>
<thead>
<tr>
<th>Security Platform</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trusted Platform Module 1.2</strong> PPI</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td><strong>Trusted Platform Module 1.2</strong> PPI</td>
<td></td>
</tr>
<tr>
<td><strong>Trusted Platform Module 1.2</strong> PPI</td>
<td>Trusted Platform Module</td>
</tr>
</tbody>
</table>

Physical Presence Interface (PPI)
<table>
<thead>
<tr>
<th>Trusted Platform Module 1.1 / PPI</th>
<th>BIOS Trusted Platform Module</th>
</tr>
</thead>
</table>

©Infineon Technologies AG
Infineon Security Platform -
## Security Platform

<table>
<thead>
<tr>
<th>Trust Domain</th>
<th>Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Platform</th>
<th>Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Platform</th>
<th>Trusted Platform Module, Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security Platform Security Platform</td>
</tr>
</tbody>
</table>
Infineon Security Platform -
Security Platform

Trusted Platform Module

- Infineon Security Platform
- Trusted Platform Module

... Security Platform

<table>
<thead>
<tr>
<th>Trust Domain</th>
<th>Security Platform</th>
</tr>
</thead>
</table>

Security Platform (SRK)

- Trusted Platform Module
- Security Platform
- Trusted Platform Module
- SRK
Technologies AG
Infineon Security Platform -
Security Platform

Security Platform

Microsoft, Trusted Platform Module (TPM) Management

Security Platform

Security Platform

Security Platform

Security Platform

OS

OS Security Platform

BIOS

OS

Security Platform

Infineon Technologies AG
Infineon Security Platform -
Security Platform

Security Platform

<table>
<thead>
<tr>
<th></th>
<th>Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>( ) Security Platform</td>
</tr>
<tr>
<td>✔️</td>
<td>BitLocker</td>
</tr>
</tbody>
</table>

BitLocker (Windows 7 Windows Vista Enterprise Ultimate edition)
Infineon Trusted Platform Module 1.2 Security Platform

Security Platform

//untranslated //untranslated
Security Platform

Trusted Computing Management Server

<table>
<thead>
<tr>
<th>Security Platform</th>
<th>XML</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPSystemBackup.xml</td>
<td></td>
</tr>
</tbody>
</table>

PC

Infineon Technologies AG
Infineon Security Platform -
Security Platform.

- Security Platform.
- Trusted Computing Management Server.
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**XML:**

**CD:**

---

Infineon Technologies AG
Infineon Security Platform -
- Trusted Computing Management Server
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>XML</td>
</tr>
<tr>
<td></td>
<td>CD</td>
</tr>
</tbody>
</table>

Infineon Technologies AG
Infineon Security Platform -
BitLocker

TPM (Trusted Platform Module) BitLocker

- BitLocker (Windows 7, Windows Vista Ultimate edition)
- BitLocker
- BitLocker

:
<table>
<thead>
<tr>
<th></th>
<th>Microsoft BitLocker</th>
</tr>
</thead>
</table>

Technologies AG
Infineon Security Platform -
<table>
<thead>
<tr>
<th>Security Platform</th>
<th>Trusted Computing Management Server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Infineon Security Platform

Infineon Security Platform Security Platform
( , EFS PSD , ) .
Security Platform ________ .

: 
• ( _______ ).
• _______ ( _______ ).
• _______ .
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Security Platform</td>
</tr>
<tr>
<td>2.</td>
<td>Security Platform</td>
</tr>
<tr>
<td>3.</td>
<td>Security Platform</td>
</tr>
<tr>
<td>4.</td>
<td>Security Platform</td>
</tr>
<tr>
<td>5.</td>
<td>Security Platform</td>
</tr>
<tr>
<td>6.</td>
<td>Security Platform</td>
</tr>
<tr>
<td>7.</td>
<td>Security Platform</td>
</tr>
<tr>
<td>8.</td>
<td>Personal Secure Drive</td>
</tr>
</tbody>
</table>

(EFS PSD)
- Security Platform
- Security Platform
- Security Platform (, EFS PSD, )
-  
- 
- 
- Windows Security Platform

<table>
<thead>
<tr>
<th>-forceinit /forceinit</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
|                      |  | Trust Domain
<p>| | |
|                      |  |</p>
<table>
<thead>
<tr>
<th>Security Platform</th>
<th>Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Platform</td>
<td>Security Platform</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
</tr>
<tr>
<td>Security Platform</td>
<td>Security Platform</td>
</tr>
<tr>
<td>Security Platform</td>
<td>Security Platform</td>
</tr>
</tbody>
</table>

©Infineon Technologies AG
Infineon Security Platform -
Infineon Security Platform -
## Security Platform

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Icon" /></td>
<td>EFS Secure Drive(PSD)</td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon" /></td>
<td>Microsoft (EFS)</td>
</tr>
<tr>
<td><img src="image3.png" alt="Icon" /></td>
<td>Personal Secure Drive</td>
</tr>
</tbody>
</table>

- **EFS**
- **PSD**
- **UNC**
- **Windows Home editions**

- **Security Platform**
: EFS / PSD

• EFS
  PSD  PSD
  PSD

• EFS  PSD  EFS  PSD
  PSD  (EFS)

• PSD (PSD).

• Security
  Platform.

Infineon Technologies AG
<table>
<thead>
<tr>
<th>URL</th>
<th>Infineon Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Infineon Security Platform</td>
</tr>
<tr>
<td></td>
<td>Infineon Security Platform</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Infineon Technologies AG
Infineon Security Platform -
• Microsoft Windows Mail/Outlook Express
• Microsoft Outlook 2003
• Microsoft Outlook XP
• Microsoft Outlook 2000
• Mozilla Thunderbird
Security Platform

Technologies AG
Infineon Security Platform -
<table>
<thead>
<tr>
<th>abcd</th>
<th>( )</th>
</tr>
</thead>
<tbody>
<tr>
<td>abcd</td>
<td>( )</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>:</td>
</tr>
</tbody>
</table>
| :   | :
| :   | Microsoft (: Windows 7 Windows Vista) :
|     | "cipher.exe"
|     | Microsoft TechNet (" " "cipher.exe").
| :   | 1024 2048
| :   | . |
Infineon Security Platform -
<table>
<thead>
<tr>
<th></th>
<th>Security Platform EFS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Documents\Encrypted Data My Documents\Encrypted Data ( )</td>
</tr>
<tr>
<td></td>
<td>desktop.ini FAT32 )</td>
</tr>
<tr>
<td></td>
<td>EFS</td>
</tr>
<tr>
<td></td>
<td>(  )</td>
</tr>
<tr>
<td></td>
<td>Security Platform EFS (Microsoft EFS)</td>
</tr>
<tr>
<td></td>
<td>Microsoft EFS</td>
</tr>
<tr>
<td></td>
<td>EFS Security Platform EFS ,</td>
</tr>
<tr>
<td></td>
<td>Microsoft EFS</td>
</tr>
<tr>
<td></td>
<td>Microsoft EFS (Security Platform )</td>
</tr>
<tr>
<td></td>
<td>EFS</td>
</tr>
<tr>
<td></td>
<td>EFS</td>
</tr>
</tbody>
</table>
Infineon Security Platform
Personal Secure Drive

Personal Secure Drive  Personal Secure Drive
Personal Secure Drive  Personal Secure Drive
Personal Secure Drive   __    .  Personal Secure Drive(PSD)

.
### Personal Secure Drive

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PSD</td>
<td>1. <strong>Personal Secure Drives</strong> 2. <strong>Personal Secure Drive</strong></td>
</tr>
<tr>
<td></td>
<td>1. <strong>Personal Secure Drives</strong> 2. <strong>Personal Secure Drive</strong></td>
</tr>
<tr>
<td></td>
<td>1. <strong>Personal Secure Drive</strong> (PSD) 2. <strong>Personal Secure Drive</strong> 3. <strong>Personal Secure Drive</strong></td>
</tr>
</tbody>
</table>

Infineon Technologies AG
Infineon Security Platform
## Personal Secure Drive

Personal Secure Drive , PSD

<table>
<thead>
<tr>
<th>Personal Secure Drive</th>
<th>Personal Secure Drive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infineon Technologies AG</td>
<td></td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>abc</td>
<td></td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

- "My Secure Drive"
- 32
- PSD

Personal Secure Drive

PSD
Infineon Security Platform
## Personal Secure Drive

<table>
<thead>
<tr>
<th></th>
<th>(MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(: USB )</td>
</tr>
<tr>
<td></td>
<td>Personal Secure Drive</td>
</tr>
<tr>
<td></td>
<td>Personal Secure Drive</td>
</tr>
</tbody>
</table>

- **PSD**
- **Personal Secure Drive**

---

<table>
<thead>
<tr>
<th></th>
<th>PSD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Personal Secure Drive</td>
</tr>
</tbody>
</table>
PSD

Personal Secure Drive

- PSD

- FAT16 PSD 2 GB.
- FAT32 PSD 4 GB.
- PSD

PSD Technologies AG
Infineon Security Platform
Personal Secure Drive

| | Personal Secure Drive
| | F5
| | PSD
| | Personal Secure Drive

| | Personal Secure Drive (PSD)
| | Personal Secure Drive

| | Personal Secure Drive
| | PSD

| | Personal Secure Drive
| | PSD

| | Personal Secure Drive
| | PSD

Infineon Technologies AG
Infineon Security Platform
## Personal Secure Drive

### Features:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personal Secure Drive (PSD)</strong></td>
<td><strong>32</strong> &quot;My Secure Drive&quot;</td>
</tr>
<tr>
<td><strong>Personal Secure Drive</strong></td>
<td><strong>PSD</strong></td>
</tr>
</tbody>
</table>

---

**Infineon Technologies AG**
Infineon Security Platform
Personal Secure Drive

Personal Secure Drive

: Personal Secure Drive

Personal Secure Drive

Personal Secure Drive

Personal Secure Drive

Personal Secure Drive

Personal Secure Drive

Personal Secure Drive

Infineon Technologies AG
Infineon Security Platform -
Infineon Security Platform

Infineon Security Platform, Infineon Security Platform

Infineon Security Platform

Infineon Security Platform

Infineon Security Platform, Infineon Security Platform

Info

- Security Platform
- Trusted Computing Management Server

Infineon Security Platform
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 1. | ?________ | Security Platform  
     |     | Security Platform  . |
| 2. | ___________ | (________). |
| 3. | _______ _______ | . |
| 4. | ______ | . |
Infineon Security Platform
|-------------------|---------------------------|---------------------------|---------------------------|

Technologies AG
<table>
<thead>
<tr>
<th>Trusted Computing Management Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>XML</td>
</tr>
</tbody>
</table>
Infineon Security Platform -
<table>
<thead>
<tr>
<th>Trusted Computing Management Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>XML</td>
</tr>
</tbody>
</table>

Infineon Technologies AG
Infineon Security Platform -
Infineon Security Platform

<table>
<thead>
<tr>
<th>Security Platform</th>
<th>Infineon Security Platform</th>
</tr>
</thead>
</table>

Infineon Security Platform

Trusted Computing Management Server

Technologies AG
Infineon Security Platform -
# Infineon Security Platform

<table>
<thead>
<tr>
<th>Type</th>
<th>Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Trusted Computing Management Server, Personal Secure Drive (PSD), Personal Secure Drive</td>
</tr>
<tr>
<td></td>
<td>Windows 7, Windows Vista</td>
</tr>
</tbody>
</table>

- Infineon Security Platform

- ID

- Security Platform

- Trusted Computing Management Server, Personal Secure Drive (PSD), Personal Secure Drive

- (: Windows 7, Windows Vista)
<table>
<thead>
<tr>
<th>PSD</th>
<th>Personal Secure Drive</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Personal Secure Drive</td>
</tr>
<tr>
<td></td>
<td>Personal Secure Drive</td>
</tr>
<tr>
<td></td>
<td>Personal Secure Drive</td>
</tr>
<tr>
<td></td>
<td>Personal Secure Drive</td>
</tr>
<tr>
<td></td>
<td>Personal Secure Drive</td>
</tr>
<tr>
<td></td>
<td>Personal Secure Drive</td>
</tr>
<tr>
<td>PSD</td>
<td>Personal Secure Drive</td>
</tr>
</tbody>
</table>

Security Platform
Infineon Security Platform -
<table>
<thead>
<tr>
<th>Infineon Security Platform</th>
<th>Infineon Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PSD(Personal Secure Drive)</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Computing</td>
<td></td>
</tr>
<tr>
<td>Management Server</td>
<td></td>
</tr>
</tbody>
</table>
Infineon Security Platform -
<table>
<thead>
<tr>
<th>Trusted Computing Management Server</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>abc</th>
<th>Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>XML</td>
</tr>
</tbody>
</table>
Infineon Security Platform -
# Personal Secure Drive

<table>
<thead>
<tr>
<th>□ abc</th>
<th>Personal Secure Drive</th>
<th>□ ...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Personal Secure Drive</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>□</td>
<td>Personal Secure Drive</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>□ ...</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

©Infineon Technologies AG
Infineon Security Platform -
<table>
<thead>
<tr>
<th>XML</th>
<th>Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Trusted Platform Module : Security Platform</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
</tr>
<tr>
<td></td>
<td>• Security Platform</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
</tr>
<tr>
<td></td>
<td>PC</td>
</tr>
<tr>
<td></td>
<td>• BIOS</td>
</tr>
<tr>
<td></td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
</tr>
<tr>
<td></td>
<td>PC</td>
</tr>
</tbody>
</table>

- Trusted Computing Management Server
## Personal Secure Drive

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### ABC Personal Secure Drive

- Personal Secure Drive
- PSD
- PSD
- PSD

### Personal Secure Drive

- Personal Secure Drive
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- PSD
- P
<table>
<thead>
<tr>
<th>Personal Secure Drive</th>
<th>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSD</td>
<td>.</td>
</tr>
</tbody>
</table>

- PSD
- PSD
- PSD
- PSD
- PSD
Infineon Security Platform -
### /Personal Secure Drive

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>abc</td>
<td>.</td>
<td>.</td>
<td>PSD</td>
</tr>
<tr>
<td>...</td>
<td>.</td>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>PSD</td>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>Personal Secure Drive</td>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>(Personal Drive).</td>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>abc</td>
<td>32</td>
<td>, &quot;My Secure Drive&quot;</td>
<td>.</td>
</tr>
<tr>
<td>✔</td>
<td>PSD</td>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>✔</td>
<td>PSD</td>
<td>.</td>
<td>.</td>
</tr>
</tbody>
</table>
Trusted Computing Management Server

| abc | / ID | ID . | ID | Infineon Technologies AG |
Trusted Computing Management Server

<table>
<thead>
<tr>
<th>abc</th>
<th>/ ID</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>ID</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>/ ID</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>ID</td>
</tr>
</tbody>
</table>

Infineon Technologies AG
Infineon Security Platform -
Security Platform

- Security Platform
- (Trusted Platform Module)
- Trusted Computing Management Server

XML

Infineon Technologies AG
Infineon Security Platform -
<table>
<thead>
<tr>
<th>abc</th>
<th>/ ID</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Trusted Computing Management Server

Infineon Technologies AG
Infineon Security Platform -
Trusted Computing Management Server
Infineon Security Platform -
Infineon Security Platform

- Security Platform
- Trusted Computing Management Server

(: Windows 7  Windows Vista)
Security Platform

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>( )</td>
</tr>
<tr>
<td>4.</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td></td>
</tr>
</tbody>
</table>
Infineon Security Platform : Infineon Technologies AG
Infineon Security Platform -
Trusted Computing Management Server

Security Platform

Infineon Technologies AG
Trusted Computing Management Server

Security Platform (Infineon Technologies AG)

.
Infineon Security Platform -
<table>
<thead>
<tr>
<th>Trusted Computing Management Server</th>
</tr>
</thead>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>abc</td>
<td>(</td>
</tr>
<tr>
<td>...</td>
<td>.</td>
</tr>
<tr>
<td>...</td>
<td>.</td>
</tr>
</tbody>
</table>

Infineon Technologies AG
Trusted Computing Management Server

Infineon Technologies AG
Infineon Security Platform -
<table>
<thead>
<tr>
<th>Security Platform</th>
<th>Trust Domain</th>
</tr>
</thead>
</table>

Infineon Technologies AG
Infineon Security Platform - PKCS #12
Infineon Security Platform PKCS #12

Infineon Security Platform PKCS #12  Personal Information Exchange
Security Platform  .

Personal Information Exchange (PKCS #12) "pfx" "p12"  .
PKCS #12  .
(CA)  .  PKCS #12
.
Microsoft

Security Platform PC:  Microsoft PKCS #12

Security Platform PC:  Security Platform PKCS #12
PKCS #12  Trusted Platform Module
<table>
<thead>
<tr>
<th></th>
<th>PKCS #12</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>PKCS #12</strong></td>
</tr>
<tr>
<td>2.</td>
<td>PKCS #12</td>
</tr>
</tbody>
</table>
Infineon Security Platform PKCS #12 Security Platform
... Security Platform (....).
# PKCS #12

PKCS #12.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="78x612" alt="Image" /></td>
<td>(:D:\certificates\MyPKCS12file.pfx D:\certificates\MyPKCS12file.p12).</td>
</tr>
<tr>
<td><img src="78x552" alt="Image" /></td>
<td>PKCS #12.</td>
</tr>
<tr>
<td><img src="78x526" alt="Image" /></td>
<td>PKCS #12.</td>
</tr>
</tbody>
</table>

---

Infineon Technologies AG
PKCS #12.

<table>
<thead>
<tr>
<th>PKCS #12</th>
<th>PKCS #12 (: \textit{Personal}).</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>PKCS #12</th>
<th>\textit{Personal} Trusted Root Certification Authorities.</th>
</tr>
</thead>
</table>

PKCS #12 (CA).
(PKCS #12).

PKCS #12.

→ \textit{Personal}.
→ CA Intermediate Certification Authorities.
→ CA Trusted Root Certification Authorities.

PKCS #12.

<table>
<thead>
<tr>
<th>PKCS #12</th>
<th>PKCS #12</th>
</tr>
</thead>
</table>

Infineon Technologies AG.
Infineon Security Platform -
## Security Platform

<table>
<thead>
<tr>
<th>Security Platform</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(TNA)</td>
<td>Security Platform</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td>:</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>Security Platform</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>Trusted Computing Management Server</td>
<td>.</td>
</tr>
</tbody>
</table>
Infineon Security Platform

<table>
<thead>
<tr>
<th>Security Platform</th>
<th>Infineon Security Platform (Security Platform)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Infineon Security Platform (Security Platform)</td>
</tr>
<tr>
<td></td>
<td>Infineon Security Platform (Security Platform)</td>
</tr>
<tr>
<td></td>
<td>Infineon Security Platform (Security Platform)</td>
</tr>
</tbody>
</table>

- Trust Domain Security Platform

- Trusted Computing Management Server
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Secure Drive -</td>
<td>Personal Secure Drive - PSD &lt; : &gt; PSD ( ). PSD ( ).</td>
</tr>
<tr>
<td>Windows PSD . PSD &lt; : &gt; PSD . PSD .</td>
<td></td>
</tr>
<tr>
<td>Personal Secure Drive - /</td>
<td>Personal Secure Drive .</td>
</tr>
<tr>
<td>Personal Secure Drive -</td>
<td>Personal Secure Drive .</td>
</tr>
</tbody>
</table>
Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.

Security Platform.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
Trusted Computing Management Server
(, "/").
```

```

:  
:  
:  
:  
:  
:  
:  
:  
:  
:  
:  
:  
```
<table>
<thead>
<tr>
<th>/</th>
<th>Trusted Computing Management Server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>:</td>
</tr>
<tr>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>• Trusted Computing Management Server</td>
</tr>
<tr>
<td></td>
<td>• (, &quot; / &quot;)</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>/</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>:</td>
</tr>
<tr>
<td></td>
<td>:</td>
</tr>
<tr>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>• Trusted Computing Management Server</td>
</tr>
<tr>
<td></td>
<td>• (, &quot; / &quot;)</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td>:</td>
</tr>
<tr>
<td></td>
<td>:</td>
</tr>
<tr>
<td></td>
<td>•</td>
</tr>
<tr>
<td></td>
<td>• Trusted Computing Management Server</td>
</tr>
<tr>
<td></td>
<td>.</td>
</tr>
<tr>
<td>Infineon TPM Strong Cryptographic Provider</td>
<td>Infineon TPM Strong Cryptographic Provider</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Infineon Security Platform</td>
<td>Infineon Security Platform</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Infineon Security Platform -
Infineon Security Platform

Trusted Platform Module
- Infineon Security Platform
- Infineon Security Platform
- Infineon Security Platform
- Infineon Security Platform
- Infineon Security Platform

Technologies AG
Infineon Security Platform  -
Infineon Security Platform


Technologies AG
Infineon Security Platform -
Infineon Security Platform

Security Platform ... ( ).

Security Platform ( ) .

Technologies AG
Infineon Security Platform -
Security Platform

Infineon Security Platform

Trusted Computing Management Server
- Windows Home editions
Security Platform


Security Platform (IfxSpPol.adm):

1. (gpedit.msc)
2. 
3. " /" .
4. " ".
6. .
1. _______  .
   (: Windows 7  Windows Vista)
   **Platform**  .
   **Security Platform**  .

2. _______  .
   _______  .
   _______  .

Microsoft    Microsoft TechNet
. Microsoft    Windows    .
F1    .

Infineon Technologies AG
Infineon Security Platform -
Infineon Security Platform

- Trusted Computing Management Server

Platform: (, ) Security
<table>
<thead>
<tr>
<th><strong>TPM</strong></th>
<th>Trusted Platform Module (PPI) Module</th>
<th>Trusted Platform Module</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trusted Computing Group (TCG)</strong></td>
<td>Security Platform</td>
<td></td>
</tr>
<tr>
<td><strong>NV</strong></td>
<td>Trusted Platform Module 1.2 (NV)</td>
<td>NV</td>
</tr>
<tr>
<td></td>
<td>NV</td>
<td>NV</td>
</tr>
</tbody>
</table>
Trusted Platform Module.

*: (Security Platform)
*: (PIN Windows BitLocker)

Infineon Trusted Platform Module
1.2 Security Platform.
Security Platform.

(S3) (S4)
Security Platform.
Security Platform.

ID(CLSID) CLSID.
<table>
<thead>
<tr>
<th>ID</th>
<th>ClassID : {76D8D888-B5AC-49FC-9408-8A45D37F3AC6}.</th>
</tr>
</thead>
</table>

**SRK**

Trusted Platform Module  Storage Root Key(SRK)  .
SRK  Security Platform

:  SRK  .
:  SRK  .

:  _______
:\BackupServer\SecurityPlatformShare\SPSystemBackup.xml.
  XML
  
SPSystemBackup.

  Security Platform PC .

:  Security Platform
  .

  (:\ServerName\FolderName\FileName.xml).

  Security Platform PC  PC

  Security Platform PC .

  .

?_____________________

  Security Platform  .

  Security Platform

  . Security Platform
- - ..._____________ .
\ServerName\FolderName\FileName.xml.

Security Platform PC            PC

Security Platform PC            .

?
<table>
<thead>
<tr>
<th>Security Platform</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Infineon Security Platform

<table>
<thead>
<tr>
<th>Information Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Computing Management Server</td>
<td></td>
</tr>
</tbody>
</table>

: (,) Security Platform.
<table>
<thead>
<tr>
<th>Security Platform</th>
<th>Infineon Security Platform (EFS, PSD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFS</td>
<td>Security Platform (EFS)</td>
</tr>
<tr>
<td>PSD</td>
<td>Security Platform Personal Secure Drive (PSD)</td>
</tr>
</tbody>
</table>

**Security Platform**

- Infineon Security Platform
- Infineon Security Platform
- Infineon Trusted Platform Module 1.1

**EFS**

- Security Platform (EFS)

**PSD**

- Security Platform Personal Secure Drive (PSD)
Security Platform

:  
  
- __________________ .

:  
  
  :  
    :  
    :  
    :  
    :  

:  
  
  :  
    :  
    :  
    :  

:  

:  

:  

:  

:  

:  

:  

:  

:  

:  

:  

:  

:  

:  

:  

:  

:  

Infineon Security Platform

:  
  
  :  
    :  
    :  
    :  
    :  

:  

URL

Security Platform ________________ .

Security Platform

:  

:  

:  

:  

• Security Platform

• 

• EFS

( EFS ).

EFS

:  

EFS .
1. **EFS**: (, )
   . 
   • : .
   • : :
   • : PC.

2. **URL**: EFS CA
   (:
   (CA) EFS
   .
   • URL .
   • EFS
   .
   • EFS Security Platform PC
     . EFS
     .
   : EFS . EFS
   ., EFS .
   :
   • EFS EFS PSD .
   • EFS (EFS PSD )
     (URL).

<table>
<thead>
<tr>
<th>EFS</th>
<th>Security Platform EFS</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(: 14 )</td>
<td></td>
</tr>
<tr>
<td></td>
<td>:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EFS</th>
<th>EFS</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10.</td>
<td></td>
</tr>
<tr>
<td><strong>Personal Secure Drive</strong></td>
<td><strong>/PSD</strong></td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td><strong>• PSD ( ) PSD</strong></td>
<td><strong>PSD</strong></td>
<td><strong>• 5000 MB</strong></td>
</tr>
<tr>
<td><strong>• PSD</strong></td>
<td><strong>• PSD</strong></td>
<td><strong>• Windows 7, Windows Vista</strong></td>
</tr>
<tr>
<td><strong>• 5000 MB</strong></td>
<td><strong>• 5000 MB</strong></td>
<td><strong>• PSD</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>• 5000 MB</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>• 5050 MB</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>• 50 MB</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>• 10 MB</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>• PSD</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>• Security Platform</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>• Security Platform</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>• MS-CAPI</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>• Infineon TPM Strong Cryptographic</strong></td>
</tr>
</tbody>
</table>

**MS-CAPI**

| **• MS-CAPI** |
| **• MS-CAPI** |
| **• MS-CAPI** |

**/ :** Infineon TPM Strong Cryptographic
Provider . Strong Cryptographic Provider .
/
.
.
: ., Infineon
TPM Strong Cryptographic Provider .
<table>
<thead>
<tr>
<th>Security Platform</th>
<th>Management Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>(, )</td>
<td>/Management Provider</td>
</tr>
<tr>
<td>(:: 2)</td>
<td>/Management Provider</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
</tbody>
</table>
Infineon Security Platform
## Security Platform

<table>
<thead>
<tr>
<th>Security Platform</th>
<th>Trusted Platform Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Crypto-API, Microsoft Cryptography Next Generation (CNG) API</td>
<td>PKCS #11 Crypto-API</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>API</th>
<th>/()</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Crypto-API</td>
<td>- EFS PSD</td>
</tr>
<tr>
<td></td>
<td>- Outlook Windows Mail/Outlook Express (S/MIME)</td>
</tr>
<tr>
<td></td>
<td>- Internet Explorer SSL/TLS</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Internet Explorer</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Office</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Crypto-API VPN</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Crypto-API</td>
</tr>
<tr>
<td></td>
<td>- Adobe</td>
</tr>
<tr>
<td>Infineon TPM PKCS #11 Provider (&quot;TPM Cryptoki Token&quot;)</td>
<td>PKCS #11 Crypto-API</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Infineon TPM Strong Cryptographic Provider(AES)</th>
<th>.</th>
<th>Microsoft Crypto-API</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>.</td>
<td>• VPN</td>
</tr>
</tbody>
</table>

| . | . | . |

<table>
<thead>
<tr>
<th>Trusted Platform Module</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Infineon TPM Platform Cryptographic Provider(Platform CSP)</th>
<th>.</th>
<th>Microsoft Crypto-API</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>.</td>
<td>• WLAN</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trusted Platform Module</th>
</tr>
</thead>
</table>

| WLAN RADIUS IEEE |
| Infineon TPM Key Storage Provider (KSP) | Key Storage Provider. Infineon TPM Cryptographic Service Provider | Microsoft Cryptography Next Generation (CNG) API API | 802.11 EAP-TLS (TLS)  
 RADIUS  
 LAN  
 IEEE  
 802.1X EAP-TLS (TLS)  
 VPN  
 IPSec |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
  
 Trusted Platform Module (CSP)  
  
  
 |  
  
 Microsoft .NET 3.0  
  
  
 |  
  
 Microsoft .NET 3.0  
  
  
 |  
  
 |  
  
 |  
  
 Microsoft .NET 3.0  
  
  
 |
Infineon Security Platform
Security Platform

Security Platform  Trusted Computing Group (TCG)  
TCG  (TSS)  

- TSS (TCG ) Service Provider
- TSS
- TSS

TCG  TCG  ,  

:  Trusted Platform Module

Infineon  Technologies AG
Server Integration Services

*Server Integration Services*  Trusted Computing Management Server

. Security Platform  Trusted Computing Management Server

( ______ ).

. Client Side Control Agent  Server Integration Service  

<table>
<thead>
<tr>
<th><strong>Client Side Control Agent</strong></th>
<th>Trusted Computing Management Server ( ______ ).</th>
</tr>
</thead>
</table>

Infineon TPM Professional Package  Server Integration Services

.

Server Integration Services  *ReadmeServerIntegrationServices.txt*

.  Client Side Control Agent  

©Infineon Technologies AG
Infineon Security Platform
Security Platform

Infineon Security Platform | Windows 2000/Windows XP
PKCS #11 | PKI
, Infineon Security Platform

- Personal Secure Drive (PSD)
- (EFS)
- Microsoft Word

Technologies AG
Infineon Security Platform
(PKI)

Security Platform
(CA) (PKI)

Security Platform / PKI

Windows (PKI)

PKCS #11

Technologies AG
Infineon Security Platform Solution
(Certificate Authority: CA)  3
  CA
  CA
Infineon Security Platform
CA
Microsoft ID . ID
VeriSign Thawte (CA)
.
CA .
•
•
•
CA . CA CA
CA .
• CA ?
• CA? CA . CA
.
• CA ?
• CA ?
• CA ?
CA CA . CA .

Security Platform .

.

Technologies AG
Infineon Security Platform
Windows (PKI)

Microsoft Windows 2000  Windows (PKI).

Windows .

PKI (DC) Kerberos Key Distribution Center(KDC)
Windows ., PKI

Microsoft PKI  Microsoft TechNet .

PKI .
  • Active Directory
  •
  •
  •

Technologies AG
Infineon Security Platform
Active Directory


CA , Active Directory PKI
Active Directory .

Active Directory ."Active Directory "
,

Active Directory Microsoft TechNet .
PKI .

Infineon Technologies AG
Infineon Security Platform
(CA) (PKI) .
 . CA
 . CA CA CA ( CA
 CA ).
Windows 2000 , , CA
 CA .
Windows 2000 CA . CA
 . CA , CA
 .
CA Windows 2000 , . , CA
 .
 Windows 2000 CA .
Windows 2000 CA .
 : CA .
Active Directory CA . CA Active
Directory DNS .
 CA Microsoft TechNet .
PKI Security Platform

Infineon

Technologies AG
Infineon Security Platform
Active Directory  (CSP)

Security Platform
Active Directory

1. **ADSI Edit**

   Active Directory Services Interface (ADSI)
   . Windows 2000 Server CD Support\Tools
   Microsoft Setup Windows 2000
   Windows 2000 CD Support\Tools Readme.doc ADSI Edit
   Microsoft Windows 2000 Resource Kit

2. **ADSI Edit**

   Adsiedit.msc(ADSI Edit MMC) .
   " " .
   mmc.exe ADSI Edit
   . ADSI Edit

3. 

   Adsiedit.msc :
   CN=< >, CN=, CN=, CN=, CN=, DC=< >.

4. 

   **CN=**User

   : pKIDefaultCSPs.

   :

   : <n>,Infineon TPM Cryptographic Provider ().

   :

   : 1,Microsoft Cryptographic Provider v1.0
   2,Microsoft Base Cryptographic Provider v1.0
   :
   3,Infineon TPM Cryptographic Provider
(CA) Security Platform.

Security Platform

Active Directory.
Infineon Security Platform
Security Platform

- Microsoft
- Microsoft Windows

Infineon Technologies AG
Infineon Security Platform
MMC (Microsoft Management Console)

CA Windows

1. Microsoft
   Microsoft

2. ...

3. 

4. Security Platform

5. Security Platform
   CSP

Security Platform

6. 

7. 

8. 

Infineon Technologies AG
Infineon Security Platform
Microsoft Windows  
Microsoft CA  

CA  

1. **Internet Explorer**  
   Internet Explorer  
   
2.  

   ![Security Platform](image)

<table>
<thead>
<tr>
<th>CSP:</th>
<th>MS V1</th>
</tr>
</thead>
<tbody>
<tr>
<td>:</td>
<td>CSP</td>
</tr>
<tr>
<td>:</td>
<td>GUID</td>
</tr>
</tbody>
</table>

Security Platform  
CSP  
GUID.
Infineon Security Platform
PKCS #11 (PKI)
PKCS #11, PKCS #11
  . PKCS #11
  .
PKCS #11
  .
PKCS #11
  .
PKCS #11
PKI
  PKCS #11
    . PKCS #11
    .
Windows 2000 / XP
  PKCS #11 3
  . Infineon Security Platform
  Trusted Platform Module PKCS #11.
  .
PKCS #11 PKCS #11
  .
    PKCS #11
    .
    .
    .
PKI
  .
  . 3
  . Infineon Security Platform PKCS #11
  .
Mozilla Firefox
PKCS#11 DLL (*ifxtpmck.dll*) Security Platform
Security Platform  PKCS#11  Security Platform

*ifxtpmck.dll*

Technologies AG
Infineon Security Platform Solution
Mozilla Firefox PKCS #11

PKCS #11 PKI .


Mozilla Firefox PKCS #11 .

Infineon Security Platform PKCS #11 Mozilla Firefox PKCS #11 .

/ .
Mozilla Firefox

1. Mozilla Firefox.
2. > ....... . .
3. 
4. 
5. . .
   . Infineon Security Platform
6. 
   ________ .
Mozilla Firefox

1. 

2. 

3. 

4. PKCS #11

5. IfxTPMCK.dll PATH

6. 

---

Infineon Technologies AG
Infineon Security Platform
Security Platform

- Sun
- PKCS #11 CA

Technologies AG
Infineon Security Platform Solution
Sun

iPlanet CA . (Windows 2000 / XP, Unix, Linux, ...).

PKCS #11 .
Mozilla Firefox

1. Mozilla Firefox
2. Mozilla Firefox
3. . .
   1025 SSL
4. .
5. . .
   •
   •
   •
   •
   :
   :
1. > ...
2.
3.
}
   .
   .
   .
   .
   .
   .
   .

Infineon Technologies AG
Infineon Security Platform
PKCS #11 CA

CA

Sun . . CA

TPM Infineon

Technologies AG
Infineon Security Platform
Personal Secure Drive

Personal Secure Drive (PSD) .
Personal Secure Drive .
Personal Secure Drive ., Personal Secure Drive ., Personal Secure Drive .
Personal Secure Drive .

1. 
2. 
<table>
<thead>
<tr>
<th>Personal Secure Drive</th>
<th>AES  RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Secure Drive</td>
<td>Personal Secure Drive</td>
</tr>
<tr>
<td>Personal Secure Drive</td>
<td>Personal Secure</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>:</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSD</td>
</tr>
<tr>
<td>PSD</td>
</tr>
<tr>
<td>.</td>
</tr>
</tbody>
</table>
PSD Trusted Computing Management Server ., PSD (  Security Platform ).
( : USB ) PSD . PSD .
( : ) PSD PSD
PSD (  Securi ). PSD  

Infineon Technologies AG
Infineon Security Platform Solution
Personal Secure Drive

Personal Secure Drive:

- AES (Advanced Encryption Standard)
- RSA
- / 
- .
Personal Secure Drive

- Personal Secure Drive:
  - : Personal Secure Drive Windows
  - Microsoft (EFS)
Trusted Platform Module

Personal Secure Drive (Trusted Platform Module (TPM))

PC "" 
Module .
Personal Secure Drive

- PC
- Trusted Platform Module
- Windows Personal Secure Drive
Personal Secure Drive

Personal Secure Drive ()

.

PSD . PSD . PSD PSD
PSD

, Personal Secure Drive - .
Personal Secure Drive )
( Personal Secure Drive ).
Windows Explorer PSD .
PSD
Windows PSD .

, Personal Secure Drive - (Personal Secure Drive ) Personal Secure Drive - < : > - (Personal Secure Drive ).
PSD

________ Personal Secure Drive .  PSD ( Personal Secure Drive )
Personal Secure Drive - < : > -
Personal Secure Drive ).
PSD

PSD  Security Platform
**PSD**

<table>
<thead>
<tr>
<th>Personal Secure Drives</th>
<th>Personal Secure Drive</th>
<th>Personal Secure Drive</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;F5&quot;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Personal Secure Drive</th>
<th>PSD</th>
<th>PSD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PSD</th>
<th>PSD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Infineon Security Platform
Personal Secure Drive

Personal Secure Drive
Personal Secure Drive    Infineon Security Platform.
Personal Secure Drive

Windows
HKEY_LOCAL_MACHINE\Software\Infineon\TPM
Software\PSD\DLSkip.

:: 7.9.9

Technologies AG
Infineon Security Platform
Personal Secure Drive


PSD
## PSD

<table>
<thead>
<tr>
<th>PSD</th>
<th>EFS Windows editions</th>
<th>EFS Windows editions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• PSD . PSD</td>
<td>• EFS . Microsoft</td>
</tr>
<tr>
<td></td>
<td>• PSD</td>
<td>• PSD PSD</td>
</tr>
</tbody>
</table>

1. **PSD**
2. PKCS #12
3. PSD

1. **PSD**
2. Microsoft EFS :
   - secpol.msc
3. **PSD**

1. **PSD**
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PSD</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
|   | PSDRecovery /V [/ID:driveID] | Microsoft EFS :
|   | : secpol.msc |   |
| PSD |   |   |
|   | : PSDRecovery secpol.msc /D:[name] [number] [/ID:driveID] | Microsoft EFS :
|   |   |   |
| PSD |   |   |
|   |   | (, PKCS #12 ..)
|   |   | Personal Secure Drive
|   |   | Personal Secure Drive
| PSD | Personal Secure Drive (* .FSF).
|   |   | * .FSF
|   |   | .
|   |   | PSD
|   |   | PSDRecovery /L
| PSD |   |   |
|   |   |   |
|   |   |   |
|   |   |   |
|   |   |   |
| end |   |   |
|   |   |   |
|   |   |   |
|   |   |   |
|   |   |   |
PSD

PSDRecovery.exe EFS cipher.exe .

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>.CER</code></td>
<td>Personal Secure Drive</td>
</tr>
<tr>
<td><code>filename.CER</code></td>
<td><code>.CER</code></td>
</tr>
<tr>
<td><code>/ID:driveID</code></td>
<td><code>: ID Personal Secure Drive</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>PSDRecovery /V</code></td>
<td>PSDRecovery /V</td>
</tr>
<tr>
<td><code>name</code></td>
<td>PSDRecovery /V</td>
</tr>
<tr>
<td><code>number</code></td>
<td>PSDRecovery /V</td>
</tr>
<tr>
<td><code>/ID</code></td>
<td>Personal Secure Drive .</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>PSDRecovery /L</code></td>
<td>Personal Secure Drive ID, . PSD</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>PSDRecovery /M:DriveImageFile.FSF [X:]</code></td>
<td>PSD</td>
</tr>
<tr>
<td><code>DriveImageFile.FSF</code></td>
<td>PSDRecovery /L PSD</td>
</tr>
<tr>
<td><code>X</code></td>
<td>.</td>
</tr>
<tr>
<td><code>()</code>.</td>
<td>.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td><code>PSDRecovery /R:filename</code></td>
<td>Windows Home editions</td>
</tr>
<tr>
<td><code>*.PFX (  ) *.CER (  )</code></td>
<td></td>
</tr>
<tr>
<td><code>filename (  )</code></td>
<td></td>
</tr>
<tr>
<td><code>PSDRecovery /V [ID:driveID]</code></td>
<td>Windows Home editions</td>
</tr>
<tr>
<td><code>Personal Secure Drive</code></td>
<td></td>
</tr>
</tbody>
</table>

**Infineon Technologies AG**
Infineon Security Platform
(EFS)

(EFS) NTFS . NTFS
 . EFS ( )

.

.

.

:

- EFS Windows Home editions .
Infineon Security Platform
EFS

- Microsoft Windows
- Microsoft EFS
- F1

- EFS TCP/IP (IPSec)
- PPTP

: EFS Windows Home editions.

Technologies AG
Infineon Security Platform
• NTFS
  Windows 2000 XP NTFS
  . NTFS .

• FAT
  FAT
  . FAT
  ( ).

•
  Windows EFS .

•
- Microsoft EFS.
- EFS

EFS . Microsoft EFS. Microsoft Windows . F1

EFS .

: EFS Windows Home editions .

Infineon Technologies AG
Infineon Security Platform
__Microsoft Windows Mail/Outlook__  __Mozilla Thunderbird__  __Infineon Technologies AG__
Infineon Security Platform
Windows Mail/Outlook Express/Outlook

·
  ·
  ·
·

Technologies AG
Infineon Security Platform
Outlook/Windows Mail/Outlook Express

- Windows Mail/Outlook Express
- Outlook 2007
- Outlook 2003
- Outlook XP
- Outlook 2000

Infineon Technologies AG
Infineon Security Platform
Windows Mail/Outlook Express
Outlook 2007
Outlook 2003
Outlook XP
Outlook 2000

Infineon Technologies AG
Infineon Security Platform
Windows Mail/Outlook Express
Outlook 2007
Outlook 2003
Outlook XP
Outlook 2000

Infineon Technologies AG
Infineon Security Platform
Mozilla Thunderbird

Mozilla Thunderbird

Technologies AG
Infineon Security Platform
Mozilla Thunderbird


Mozilla Thunderbird

1. Mozilla Thunderbird.
2. > ...
3.
4. ...
   ()
5.
A. ( )
B. ( )

PKCS #11 Mozilla Firefox_PKCS #11.

Technologies AG
Infineon Security Platform
Mozilla Thunderbird

1. Mozilla Thunderbird.
2. > >
3. 
4. 
5. 
6. > 

Technologies AG
Infineon Security Platform
Mozilla Thunderbird

1. Mozilla Thunderbird.
2. > > .
3. .
4. .
5. .
6. > .
   . .
Infineon Security Platform Solution
Microsoft Word
Microsoft Word

Microsoft Word 2000 Microsoft Word XP.

Technologies AG
Infineon Security Platform
Microsoft Word

Microsoft Word

Microsoft Word

Microsoft Word

Technologies AG
Infineon Security Platform
Microsoft Word

1. >>... .

2. : //.
1.  

2.  >> ....  (Microsoft Word 2007 : >> ...

3.  

4.  

5.  

6.  .
Microsoft Word 2007

1. 
2. > > ,  
3.  
4. Visual Basic  
5. Project Explorer  
6. Visual Basic > ...  
7. ...  
8.  
9.  
10.  
11.  
12. Word : Microsoft Word  
13. > Microsoft Word  
1. 
2. >> 
3. , , .
   : Visual Basic >> Visual Basic Editor .
5. 
6. Visual Basic > ... .
7. 
8. .
9. .
10. .
11. .
12. .
13. .
   : (Normal.dot ) .

Microsoft Word .
<table>
<thead>
<tr>
<th>Security Platform</th>
<th>Provider Details</th>
<th>Protocol(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>/ ()</td>
<td>Infineon TPM Cryptographic Provider</td>
<td>SSL/TLS</td>
</tr>
<tr>
<td></td>
<td>Infineon TPM RSA AES Cryptographic Provider (CSP)</td>
<td></td>
</tr>
<tr>
<td>/ ()</td>
<td>Infineon TPM PKCS #11 Provider</td>
<td>SSL/TLS</td>
</tr>
<tr>
<td>VPN</td>
<td>Infineon TPM Cryptographic Provider</td>
<td>IPsec</td>
</tr>
<tr>
<td></td>
<td>Infineon TPM RSA AES Cryptographic Provider (CSP)</td>
<td></td>
</tr>
<tr>
<td>VPN</td>
<td>Infineon TPM Platform Cryptographic Provider (Platform CSP)</td>
<td>IPsec</td>
</tr>
<tr>
<td>WLAN LAN</td>
<td>Infineon TPM Cryptographic Provider</td>
<td>WLAN: IEEE 802.11 EAP-TLS, LAN: IEEE 802.1X EAP-TLS</td>
</tr>
</tbody>
</table>
|                  | Infineon TPM Platform Cryptographic Provider (Platform CSP) | WLAN: IEEE 802.11 EAP-TLS  
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN LAN</td>
<td>Infineon Technologies AG</td>
<td>LAN: IEEE 802.1X EAP-TLS</td>
</tr>
</tbody>
</table>
IIS Active Directory
Internet Explorer
Mozilla Firefox PKCS #11

- IIS Active Directory
- Internet Explorer
- Mozilla Firefox
- Mozilla Firefox

Infineon Technologies AG
Infineon Security Platform
Internet Explorer

Internet Explorer

Microsoft TechNet.

Infineon Technologies AG
Infineon Security Platform
IIS  Active Directory

Internet Information Services(IIS) .

IIS  Active Directory  .
Active Directory  .  IIS

:  IIS  Secure Sockets Layer(SSL) .
CA  .  SSL

"IIS  Active Directory  "  "Internet Information Service"
Microsoft TechNet .

Technologies AG
Infineon Security Platform Solution
Infineon Security Platform Solution
Mozilla Firefox

:  ( )

: SSL (Secure Sockets Layer) CA
: SSL

Infineon Technologies AG
Infineon Security Platform Solution
(VPN)
VPN ().
VPN "".
(VPDN), 'LAN' .
, VPN
(ESP) . ESP (NAS).

Technologies AG

©Infineon
Infineon Security Platform Solution
(EAP)
(EAP) (Virtual Private Network)
.
EAP VPN  EAP
  (VPN)
.
EAP (CA)  Security Platform  VPN
EAP  (X.509)
EAP  VPN

Infineon Security Platform Solution  
  .  Trusted Platform Module  .

VPN  Microsoft TechNet  Microsoft VPN  .
Microsoft  Windows  .  F1
.
(VPN)  .  VPN  VPN
.
EAP  .  VPN
  .  Microsoft Windows
Microsoft TechNet  .
  EAP  .
  •  VPN  .
  •  SmartCard
   (EAP)  .
  •  EAP  .

EAP  .

Technologies AG
Infineon Security Platform
LAN(WLAN)


WLAN .
WLAN

LAN(WLAN) .
WLAN .
() . LAN .

IEEE 802.11(, "Wi-Fi") LAN .
Wi-Fi Protected Access( WPA) Wired Equivalent Privacy( WEP) .
WLAN

- Microsoft Developer Network (MSDN)
- Microsoft Windows ("")
- Wi-Fi
- LAN (WLNA)
Security Platform  WLAN

- WLAN  WLAN  Trusted Platform Module  Security Platform PC.
- Security Platform .

WLAN

Infineon  Technologies AG
Infineon Security Platform
WLAN
WLAN . LAN(IEEE 802.1X) Security Platform
(Cryptographic Service Provider ) WLAN .
<table>
<thead>
<tr>
<th></th>
<th>WLAN Security Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>WLAN Security Platform</td>
</tr>
<tr>
<td>2.</td>
<td>WLAN</td>
</tr>
<tr>
<td>3.</td>
<td>WLAN Security Platform</td>
</tr>
</tbody>
</table>
WLAN

WLAN RADIUS

CSP (Infineon TPM Cryptographic Provider
Infineon TPM RSA and AES Cryptographic Provider).
CSP (Infineon TPM Platform Cryptographic Provider).
CSP Administrators.
WLAN

WLAN  WLAN  .  WLAN

.  .  .  WLAN

• Microsoft Windows (" ") WLAN

•
  - IEEE 802.1x .
  - EAP .
  -

.Administrators .
WLAN

• Microsoft Windows (" ") WLAN .
• " " .
Infineon Security Platform
Infineon Security Platform
(FAQ)

Infineon Security Platform  

Infineon Security Platform

Internet Explorer . .

EFS

EFS

Infineon Security Platform

Infineon Security Platform

EFS Windows editions EFS

Infineon Security Platform

Windows .

Infineon Security Platform

Security Platform

Infineon Security Platform

↓
Infineon Security Platform

i) Windows 7 Vista: \%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\RestoreData\<Machine SID>\Users\<User SIDs>\SHTempRestore.xml

ii) Windows XP Professional, Windows 2000:
\%ALLUSERSPROFILE%\Application Data\Infineon\TPM Software 2.0\RestoreData\<Machine SID>\Users\<User SIDs>\SHTempRestore.xml

i) Windows 7 Vista: \%ALLUSERSPROFILE%\Infineon\TPM Software
2.0\PlatformKeyData
IFXConfigSys.xml
IFXFeatureSys.xml
TCSps.xml
TPMCPSys.xml

ii) Windows XP Professional, Windows 2000:
%ALLUSERPROFILE%\<Application Data>\Infineon\TPM Software 2.0\PlatformKeyData
IFXConfigSys.xml
IFXFeatureSys.xml
TCSps.xml
TPMCPSys.xml

i) Windows 7 Vista:
%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\BackupData\<Machine SID>\System\SHBackupSys.xml
%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\BackupData\<Machine SID>\Users\<User SIDs\SHBackup.xml

ii) Windows XP Professional, Windows 2000:
%ALLUSERSPROFILE%\<Application Data>\Infineon\TPM Software 2.0\BackupData\<Machine SID>\System\SHBackupSys.xml
%ALLUSERSPROFILE%\<Application Data>\Infineon\TPM Software 2.0\BackupData\<Machine SID>\Users\<User SIDs\SHBackup.xml

:   \%AppData%\Infineon\TPM Software 2.0\UserKeyData\TSPps.xml

TPM Cryptographic Service Provider:   \%AppData%\Infineon\TPM Software 2.0\UserKeyData\TPMcp.xml

TPM PKCS #11:   \%AppData%\Infineon\TPM Software 2.0\UserKeyData\TPMck.xml

:   \%AppData%\Infineon\TPM Software 2.0\UserKeyData\ IFXConfig.xml
IFXFeature.xml

:
HKEY_LOCAL_MACHINE\SOFTWARE\Infineon\TPM Software
HKEY_CURRENT_USER\Software\Infineon\TPM software
**Personal Secure Drive**

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Infineon\TPM Software\PSD]
[HKEY_CURRENT_USER\SOFTWARE\Infineon\TPM Software\PSD]
```

**Personal Secure Drive**

```
x:\Security Platform\Personal Secure Drive\System Data
x: Personal Secure Drive . Personal Secure Drive
   Personal Secure Drive .
```

```
: Trusted Platform Module
(: C:\WINDOWS\Tasks\Security Platform Backup Schedule)
```

**Internet Explorer**

```
Internet Explorer . Internet Explorer
```

```
Cryptographic Service Provider
```

**Infineon Security Platform**

```
Infineon Security Platform
```

```
Infineon Security Platform
```
Infineon Security Platform

Security Platform

Trusted Computing Management Server

??
Script GeneratePubKeyArchive.vbs:
'GeneratePubKeyArchive.vbs <Full path to Token.xml> <Full path to PubKeyArchive.xml>
'<Full path to Token.xml> : 
' - SPPwdResetToken.xml
' - SPEmRecToken.xml
' - SPGenericToken.xml
'<Full path to PubKeyArchive.xml> :
' - SPPwdResetTokenPubKeyArchive.xml
' - SPEmRecTokenPubKeyArchive.xml
' - SPGenericTokenPubKeyArchive.xml
"" " :
' - SPEmRecTokenPubKeyArchive.xml
' - SPGenericTokenPubKeyArchive.xml
"" " :
' - SPPwdResetTokenPubKeyArchive.xml
' - SPGenericTokenPubKeyArchive.xml
', :
'GeneratePubKeyArchive.vbs "c:\tmp\SPGenericToken.xml"
"c:\tmp\SPGenericTokenPubKeyArchive.xml"
If WScript.Arguments.Count <> 2 Then
    WScript.Echo " : " & Wscript.ScriptName & " " "<Full path to Token.xml>" " "<Full path to PubKeyArchive.xml>""
    WScript.Quit
End If
Set MPBase = WScript.CreateObject("IIfxSpMgtPrv.MgmtProvider")
Set MPToken = MPBase.GetInterface(10)
' CreationFlags: keep existing file = 0, overwrite existing file = 1
CreationFlags = 0
ReservedFlag = 0
MPToken.CreatePublicKeyFile WScript.Arguments(0), WScript.Arguments(1),
CreationFlags, ReservedFlag
'Error Handling if failing to be added here
WScript.Echo ""

⚠️ Trusted Computing Management Server
Infineon Security Platform
Infineon Security Platform

Trusted Platform Module.

Windows Home editions EFS

EFS.

Security Platform

Security Platform.

Infineon Security Platform

Infineon Security Platform.

EFS

EFS.

EFS.

Infineon Security Platform.

Infineon Security Platform.

EFS.

EFS.

Trusted Platform Module.

Security Platform

Security Platform.

Infineon

Security Platform ("", SRK) Trusted Platform Module

Security Platform ( ).

Trust Domain.

Security Platform Trust Domain ( ).
Infineon Security Platform

Trust Domain

Trusted Platform Module

(Infineon TPM Professional Package

Trusted Domain, Windows Vista

TPM) Management

Infineon Security Platform

ID(SID)

Trusted Computing Management Server

EFS

Infineon Security Platform
Infineon Security Platform  EFS

EFS  .  ?

EFS

:    .  Infineon Security Platform

Windows 2000  :  Security Platform

Infineon Technologies AG
Infineon Security Platform -
Infineon Security Platform
MMC (Microsoft)

- MMC Security Platform
- Trusted Platform Module
- (EFS) Personal Secure Drive (PSD)
PKCS #12.

: Security Platform

: Trusted Platform Module

: EFS PSD

(CA)
EFS:

- ...
  (CA).
- CA.
- EFS PSD.

... EFS.
EFS EFS PSD.

---

URL.

---
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>i</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PC</td>
<td>(:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EFS PSD  .</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PKCS #12</td>
<td>. Security Platform</td>
</tr>
<tr>
<td></td>
<td>PKCS #12</td>
<td>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trusted Platform Module .</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Infineon TPM Cryptographic Provider</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PKCS #11</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PKCS #11</td>
<td>Security Platform .</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trusted Platform Module</td>
<td></td>
</tr>
</tbody>
</table>
Microsoft

PC

EFS PSD

Trusted Platform Module

(CA)

EFS

Security Platform

(CA) CA

EFS

EFS PSD
<table>
<thead>
<tr>
<th>EFS</th>
<th>PSD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>.</td>
</tr>
</tbody>
</table>
Security Platform (----------)

Security Platform EFS PSD
... (----------).
Infineon Security Platform -