

**Infineon Security Platform**



# Infineon Security Platform

Security Platform Trusted Platform Module

Web

<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 PKCS #12
- Security Platform
- Security Platform
- Security Platform
- Security Platform
- Server

- Personal Secure Drive

[Infineon Security Platform](#) Infineon Trusted Platform Module Infineon Security Platform

- [.](#)
- [\\_\\_\\_\\_\\_](#)
- [\\_\\_\\_\\_\\_](#)

- [Internet Information Server Active Directory](#)
- [Internet Explorer Mozilla Firefox](#)
- [Microsoft Word](#)

1 [\\_\\_\\_\\_\\_](#) Security Platform

---

Technologies AG



©Infineon

**Infineon Security Platform**

# Trusted Platform Module

e-  
**Computing Group** TCG  
**Trusted Platform Module (TPM)**

**TCG (Trusted**

Trusted Platform Module PC

Trusted Platform Module (PKI : Public Key Infrastructure)

TCG Trusted Platform Module  
Infineon Trusted Platform Module RSA  
(SHA-1 MD-5) (True Random Number Generator)  
Trusted Platform Module SPA (simple power analysis) DPA  
(differential power analysis)

Infineon Security Platform

---

Technologies AG



# **Infineon Security Platform**



# Microsoft Windows

Microsoft Windows

# (UAC)

Windows Vista IT  
"" Windows

Windows (: [Infineon Security Platform](#) Security Platform  
)



- Windows 7
- Windows

# Microsoft BitLocker

Windows Vista Microsoft

[BitLocker](#)

BitLocker Trusted Platform Module

Trusted Platform Module Trusted Platform Module

[Infineon Security Platform](#)

[Infineon Se](#)

(TPM) :

Microsoft *(TPM)*  
Trusted Platform Module Microsoft TechNet  
Microsoft TechNet

Windows Vista

# Windows Vista

TPM TSS Windows Vista TPM Windows

---

Technologies AG



## **Infineon Security Platform -**

## Server Security Platform Trust Domain

### *Trusted Computing Management Server*

	<ul style="list-style-type: none"><li>• Trust Domain ( <i>Trusted Computing Management Server</i> )</li><li>• Trusted Platform Module</li><li>• Trusted Platform Module (Infineon TPM Professional Package Trusted Domain Server Windows (TPM) )</li><li>• Trust Domain Trust Domain</li></ul>
	<ul style="list-style-type: none"><li>• Trust Domain ( <i>Trusted Computing Management Server</i> )</li><li>• Trusted Platform Module</li><li>• Trust Domain Trust Domain</li><li>•</li></ul>

Security Platform Trust Domain



:  
:  
:

<a href="#">_____</a>	Security Platform Security Platform	Security Platform Trusted Computing Management Server
<a href="#">_____</a> <a href="#">_____</a>	( _____ )	Trusted Computing Management Server
<a href="#">_____</a>	() Security Platform	Trust Domain Security Platform
<a href="#">_____</a> <a href="#">_____</a>	Security Platform <a href="#">Platform</a>	Trusted <a href="#">Security</a> Computing Management Server
<a href="#">_____</a>		Trusted Computing Management Server
<a href="#">_____</a> <a href="#">_____</a>	Personal Secure Drive (PSD)	Server Personal Secure Drive (PSD)
<a href="#">_____</a> <a href="#">_____</a> <a href="#">_____</a>		Trusted Computing Management Server
<a href="#">PKCS</a> <a href="#">#12</a> <a href="#">_____</a> <a href="#">_____</a>	Personal Information Exchange Security Platform	



# **Infineon Security Platform**

# Infineon Security Platform

Infineon Security Platform



*ReadmeUpgrade.txt*

## 1. Setup

Infineon Security Platform

## 2. InstallShield Infineon Security Platform

## 3. (EULA)

## 4. EULA

## 5.

## 6.

## 7.

- 

- 

## 8.

Infineon Security Platform

## 9.

## 10.

## 11. InstallShield Infineon Security Platform

- 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 Provider
- Security Platform
- Trusted Platform Module
- Server

12. Infineon Security Platform

13. **TPM** ( Trusted Platform Module Physical Presence Interface ) Trusted Platform Module

14. **Readme**

15.



©Infineon Technologies AG

**Infineon Security Platform**

# Infineon Security Platform

Infineon Security Platform (Disabled) Infineon Security Platform ()

Infineon Security Platform Infineon Security Platform

Infineon Security Platform

- Infineon Security Platform Infineon Security Platform

- Infineon Security Platform



Trust Domain Security Platform

- Infineon Security Platform Infineon Security Platform

## [Infineon Security Platform](#)

Infineon Security Platform Infineon Security Platform  
[Trusted Platform Module](#)

Infineon Security Platform

Security Platform [FAQ \(\)](#)



©Infineon Technologies AG

# **Infineon Security Platform**



Security Platform :

- Security Platform Windows ( )  
Windows
- 
- Security Platform
- ( )
- 1

<b>Security Platform</b>	Windows ( )	Security Platform	Security Platform Windows Security Platform	
<b>Security Platform</b> ( "" )	Windows ( )	Windows		Windows
<b>Security Platform</b> ( " " )	Windows ( )	Security Platform  Security Platform	Security Platform Windows Security Platform	
<b>EFS/PSD</b> ( " )		EFS/PSD  EFS PSD	EFS/PSD	

)



© Infineon Technologies AG

# **Infineon Security Platform**

Infineon Security Platform  
Security Platform

Infineon Security Platform 2



PIN

USB

'''

PIN  
PIN PIN

:

Security Platform 2 :

- 
-

Security Platform

Security Platform





-	
1.	
2.	Security Platform : _____ Security Platform : - _____ - ... _____
-	
3. Security Platform	: _____ : - - ... _____







# **Infineon Security Platform**

# Security Platform

Infineon Security Platform ( ) Security Platform Security Platform

## Security Platform

	...	/
		<p>() (TPM) "</p> <p> _____ Trusted Computing Management Server</p>
	/	<p>Security Platform Security Platform Personal Secure Drive Trusted Platform Module</p> <p> _____ Security Platform Trusted Computing Management Server</p>
		<p>Security Platform ( <a href="#">Security Platform</a> ) (Trusted Platform Module )</p> <p> _____ Security Platform Trusted Computing Management Server</p>
		<p>Security Platform</p> <p> _____ Trusted Computing Management Server</p>

/		Security Platform ( <a href="#">_____</a> ) 1 <a href="#">Securi</a>
		Security Platform   <a href="#">_____</a> Trusted Computing Management Server
		Security Platform
	/	 <a href="#">_____</a> Trusted Computing Management Server
PKCS #12 (Personal Information Exchange )		



**Infineon Security Platform**

Security Platform

Security Platform

EFS PSD

—

—

---

Technologies AG



# **Infineon Security Platform**

# Security Platform

Security Platform Trusted Platform  
Module Security Platform Security Platform

Personal Secure Drive Security Platform  
(: ) Security Platform



- \_\_\_\_\_ Personal Secure Drive(PSD)  
TrustedComputing Management  
Server
- Trusted Computing Management Server \_\_\_\_\_



## Security Platform

<b>Security Platform</b>	
	Security Platform
	Security Platform
	<ul style="list-style-type: none"> <li>• (" "): SPSysSystemBackup.xml SPSysSystemBackup ): Security Platform (1 Security Platform ) Security Platform ID ID</li> <li>• (: SPBackupArchive.xml): Security Platform (1 Security Platform ) 1 Security Platform ID ID</li> </ul>
<b>Security Platform</b>	
	Security Platform
	Trusted Platform Module Security Platform Security Platform
	<ul style="list-style-type: none"> <li>•</li> <li>• (: SPEmRecToken.xml) / SpToken_&lt;PCName&gt;.xml): Security Platform (:</li> </ul>
<b>Personal Secure Drive</b>	
	PSD
	PSD PSD :

- PSD
- PSD PSD

[Personal Secure Drive](#)

- PSD
- **PSD**  
Security Platform

(: SpPSDBackup.fsb): PSD

(" ")	0 <hr/>
	Personal Secure Drive (PSD) <hr/>

	Security Platform Personal Secure Drive
Trusted Platform Module	
Security Platform	Security Platform Personal Secure Drive

(" ")

: (Security  
Platform PSD )

Security Platform :

### Security Platform

:

- Infineon Security Platform

- **Security Platform**

- 

- 

- ()

- 

- XML (:

- SPSsystemBackup.xml)

- (: SPSsystemBackup) :

- \%ALLUSERSPROFILE%\My  
Documents\Security Platform

- 12:00

...

- 

- (:

- **SPEmRecToken.xml)**

- 

- 

- 

- Security Platform

Security Platform : -  
- ...

:

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

...

- 
- 

- Security Platform





\_\_\_\_\_ Trusted  
Computing Management Server

("")

:

:

- Infineon Security Platform
- -  
- ...
- ...
- ...  
(:  
**SPBackupArchive.xml**)
- Personal Secure Drive

	<p>(<a href="#">Personal Secure Drive</a>)</p> <ul style="list-style-type: none"> <li>•</li> <li>•</li> </ul> <p> <a href="#">Personal Secure Drive (PSD)</a> Trusted Computing Management Server Personal Secure Drive (PSD)</p>
<p>⋮</p> <p>⋮</p> <p></p>	<p><a href="#">- - ...</a></p>
<p>(""")</p>	
<p>⋮</p>	<p>⋮</p> <ul style="list-style-type: none"> <li>• Infineon Security Platform <a href="#">-</a></li> <li>• <a href="#">- ...</a></li> <li>• ... ( : SPBackupArchive.xml)</li> <li>•</li> <li>•</li> <li>•</li> <li>• Personal Secure Drive Personal Secure Drive (<a href="#">Personal Secure Drive</a>)</li> </ul>

- 
- 
- Security Platform  
**Security Platform**

- 
- - Security  
**Platform**
- Personal Secure  
Drive (PSD)



\_\_\_\_\_ Personal Secure  
Drive (PSD)  
Trusted Computing Management  
Server



- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_ Security Platform



©Infineon Technologies AG

# **Infineon Security Platform**

Infineon Security Platform

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

Infineon Security Platform Infineon  
Platform Infineon Security Platform Infineon  
Security Platform () Security Platform

[Security Platform](#) \_\_\_\_\_ [Security Platform](#) \_\_\_\_\_

[Security Platform](#) \_\_\_\_\_




\_\_\_\_\_ Personal Secure Drive (PSD)  
Trusted Computing Management Server

---

Trusted Platform Module  
Security Platform Security Platform  
Security Platform

---



(Trusted Platform Module )Security  
Platform

()

---

Security Platform *SpUserWz.exe /forceinit*

- 
- : *SpUserWz.exe /forceinit*

**Infineon Security Platform**

## Trusted Platform Module Infineon Security Platform 2

### Security Platform :

- Infineon Security Platform (Trusted Platform Module Security Platform )



\_\_\_\_\_ Trust Domain Trusted Platform Module  
Trusted Computing Management Server

### Security Platform :

- 



:

- : Security Platform
- : Security Platform
- \_\_\_\_\_ Trusted Computing Management Server  
Personal Secure Drive (PSD)

<b>1 - Trusted Platform Module</b>	
1 Trusted Platform Module BIOS () ( )Infineon Security Platform	
<b>2 - Security Platform</b>	:
Trusted Platform Module Security Platform	Infineon Security Platform Infineon Security Platform <u>Security</u> <u>Platform</u>

<b>Infineon Security Platform</b>	:
Infineon Security Platform Infineon Security Platform	<a href="#"><u>Security Platform</u></a>



©Infineon Technologies AG



# **Infineon Security Platform**

( )

( ) Windows

- ( )Trusted Computing Management Server ( )

- 

- ( )

- ( )



- Personal Secure Drive

- 



©Infineon

Technologies AG

**Infineon Security Platform**

# EFS PSD

EFS PSD :

- 
- 
- (EFS PSD )
- 

EFS Microsoft TechNet

PSD , [Personal Secure Drive](#)



©Infineon Technologies AG

# **Infineon Security Platform**

# Infineon Security Platform

0

## Infineon Security Platform

### Infineon Security Platform

2

## 2 Infineon Security Platform

### Infineon Security Platform Trusted Platform Module



\_\_\_\_\_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  
2 Personal Secure Drive  
Personal Secure Drive ( \_\_\_\_\_)Personal Secure Drive

*Personal Secure Drive*

- PSD PSD  
PSD (



©Infineon Technologies AG



# **Infineon Security Platform**

2



Trusted Computing Management Server  
( 3 4 )

1 -

()  
(  
Trusted Platform Module  
)

Infineon Security Platform

()

:

- Infineon Security Platform

• ...

•

**SpPubKeyArchive.xml**

:

2 -

(  
1) Infineon Security  
Platform

() Infineon  
Security Platform

:

- Infineon Security Platform

• ...

• ...

•

**SpPubKeyArchive.xml**

•

**OK**

- ID

1 2 -

2 1

2 Infineon Security Platform 2

(DCOM ) Infineon Security Platform  
Infineon Security Platform

- (Infineon Security Platform )
- Infineon Security Platform
- 
- *SRK*
- DCOM (Microsoft Windows XP )
- DCOM
- 

(1 2)

() Infineon Security Platform

:

- Infineon Security Platform
- ...
- ...
- **OK**
-



Personal Secure Drive Personal Secure Drive  
PSD :  
**SpPSDBackup.fsb)** PSD

1 -

Infineon Security Platform  
(  
)

Infineon Security  
Platform  
:

- Infineon Security Platform

- ...

- 

- 

- **SpMigrationArchive.xml**

- 

- 

- 


PSD

2 -

""

Infineon Security  
Platform  
:

- Infineon Security Platform

	<ul style="list-style-type: none"> <li>• ...</li> <li>• <b>SpMigrationArchive.xml</b></li> <li>•</li> <li>•</li> <li>• Security Platform</li> <li>•</li> <li>• <b>Security Platform</b></li> </ul> <p> <a href="#">Personal Secure Drive</a></p>
--	---

**3 -**

	<p>:</p> <ul style="list-style-type: none"> <li>• Infineon Security Platform</li> <li>• ...</li> <li>• Security Platform</li> <li>-</li> <li>• <b>OK</b></li> </ul>
--	---

**4 - –Personal Secure Drive**

<p>Personal Secure Drive</p>	<p>1 Personal Secure Drive Personal Secure</p>
------------------------------	--

Drive ( [Secure Drive](#) )Personal  
Secure Drive *P*  
*Secure Drive*  
Personal Secure Drive  
  
(:  
**SpPSDBackup.fsb)**  
2 Personal Secure  
Drive



# **Infineon Security Platform**



Infineon Security Platform

Infineon Security Platform  
Security Platform



Trusted Computing Management Server

Security Platform  
Security Platform

Security Platform

Security Platform

## 2 Security Platform

### Security Platform

1. :



\_\_\_\_\_

Security Platform :

:

- Infineon Security Platform

- 

- 

- 

(:  
**SPPwdResetToken.xml)**

:

- 

- 

- 

Security Platform : - \_\_\_\_\_

- ...

:

- Infineon Security Platform

- ...

- 

- 

(:  
**SPPwdResetToken.xml)**

:

2. :



- 
- 
- 

:

:

- Infineon Security Platform

- 

- (: **SPPwdResetSecret.xml**)

- 

- Security Platform

- 

:

...

:

- Infineon Security Platform

- ... **OK**

- (: **SPPwdResetSecret.xml**)

- 

- 

- 

-

3. :  
1

- - ... (  
)  
:  
• Infineon Security Platform  
• ...  
• (  
: **SPPwdResetToken.xml**  
• (  
: **SPPwdResetCode.xml**  
(:  
)  
•  
:  
• Infineon Security Platform  
• ...  
• (  
: **SPPwdResetToken.xml**  
• (:  
**SPPwdResetSecret.xml**)  
•  
•  
•

4. :  
( )

- - ...  
( )

:

- Infineon Security Platform
- ...
- (: SPPwdResetSecret.xml)
- ( : **SPPwdResetCode.xml**)
- 
- 
- 





# **Infineon Security Platform**



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

Security Platform  
TCG 1.2 Security Platform



•  
• ( )  
•

## Security Platform

- 
- 
- Microsoft
- 
- 
- ( )

## Security Platform



Technologies AG



©Infineon

# **Infineon Security Platform**

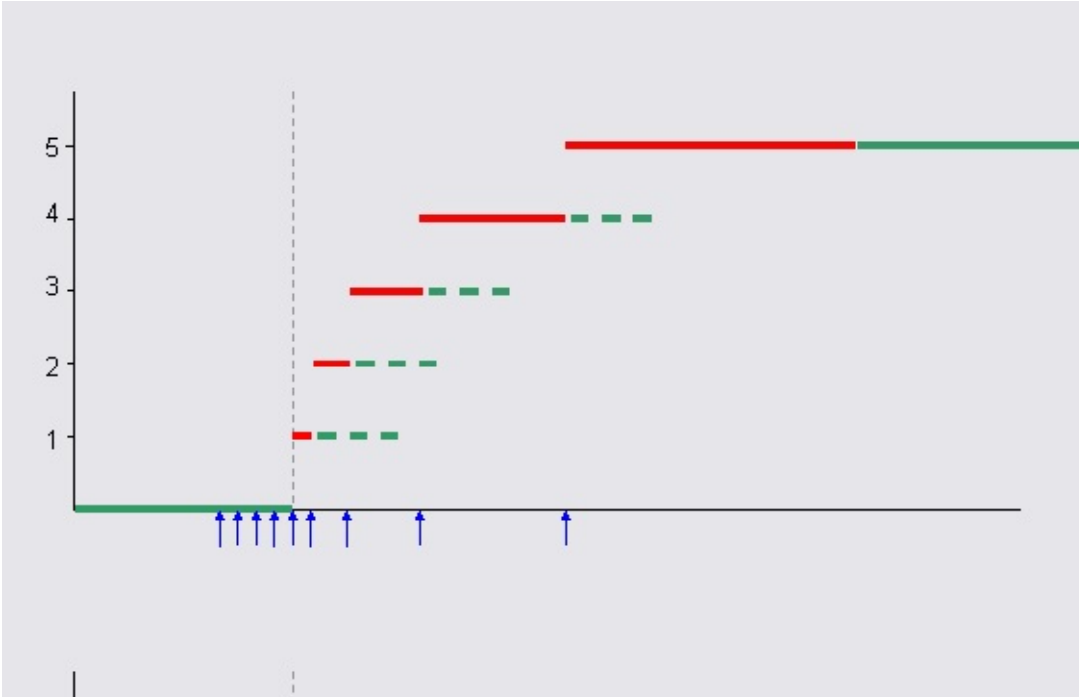


- Trusted Platform Module 1.2 Security Platform  
Security Platform Infineon Trusted Platform Module 1.2  
Security Platform
- Security Platform

### Security Platform

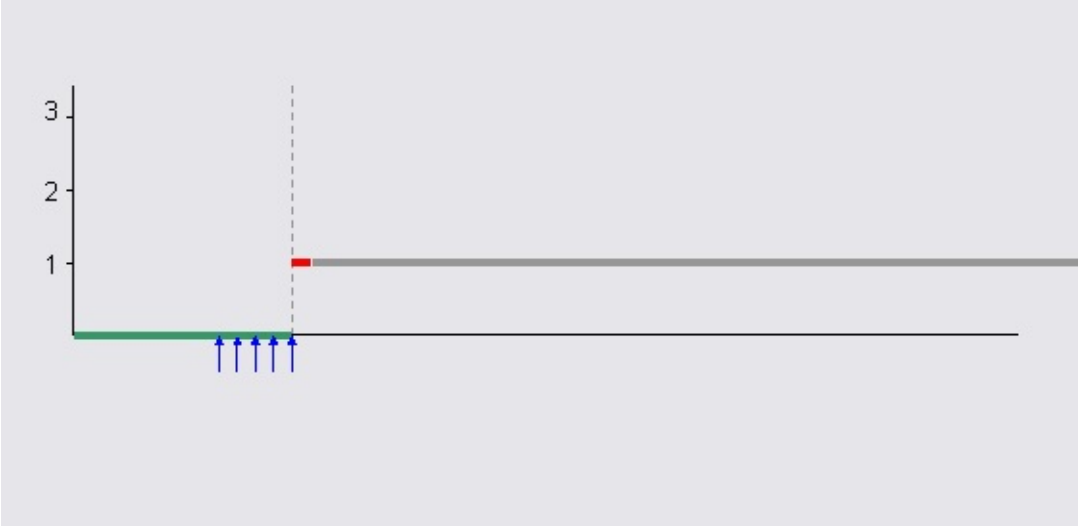
- Security Platform Platform Security Platform Security
- :
- 
- Security Platform

# Security Platform



# Security Platform

Security Platform



Security Platform Security Platform





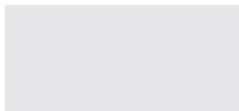
Security Platform



( ) ( ) Security Platform

## Infineon Trusted Platform Module Trusted Platform Module

(: Security Platform )	5	6 5 ( )
Security Platform	3	6 3 ( )
(: Windows BitLocker PIN )	10	6 10 ( )
	~10	10
	~24	24 15
	~6	6 1 6 1



# **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  
*SpTPMWz.exe* *-resetattack*



Security Platform

\_\_\_\_\_:

Trusted Computing Management Server

- 
- Trust Domain Trust Domain



*-resetattack* */resetattack* Security Platform  
*SpTPMWz.exe* Security Platform

:

- (Security Platform Security Platform )

•

•

()



©Infineon Technologies AG

# **Infineon Security Platform**



:

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



:

- 

<input checked="" type="checkbox"/> <i>Security Platform</i>	<p>Security Platform</p> <p>:</p> <ul style="list-style-type: none"> <li>•</li> <li>• (: Security Platform )</li> <li>• (: Windows BitLocker PIN )</li> </ul> <p>Security Platform Trusted Computing Group (TCG) Trusted Platform Module Security Platform</p>
	1
<input checked="" type="checkbox"/>	Security Platform






# **Infineon Security Platform**



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

Security Platform

<p><b>1.</b></p>	<pre> :   : : : • : Trusted Platform Module   _____ """) •   : •   : (           ) : "F5" : 0 0  Trusted Platform Module </pre>
<p><b>2. Security Platform</b></p>	<ul style="list-style-type: none"> <li>•</li> </ul>



# **Infineon Security Platform**

# Infineon Security Platform



Security Platform

## Infineon Security Platform

Security Platform	
<a href="#">Security Platform</a>	<ul style="list-style-type: none"> <li>Trusted Platform Module</li> <li>Infineon Security Platform</li> </ul>
<a href="#">Security Platform</a>	<ul style="list-style-type: none"> <li>Infineon Security Platform ( )</li> </ul>
<a href="#">Security Platform</a>	<ul style="list-style-type: none"> <li>Infineon Security Platform</li> </ul>
<a href="#">Security Platform</a>	<ul style="list-style-type: none"> <li>Infineon Security Platform</li> </ul>
<a href="#">Security Platform</a>	<ul style="list-style-type: none"> <li>Infineon Security Platform Infineon Security Platform Infineon Security Platform</li> </ul>
<a href="#">Security Platform</a>	<ul style="list-style-type: none"> <li>Security Platform</li> </ul>
<a href="#">Security Platform</a>	<ul style="list-style-type: none"> <li></li> </ul>
<a href="#">Security Platform PKCS #12</a>	<ul style="list-style-type: none"> <li>PKCS #12 (Personal Information Exchange) Security Platform</li> </ul>
<a href="#">Security Platform</a>	<ul style="list-style-type: none"> <li></li> </ul>
<a href="#">Security Platform</a>	<ul style="list-style-type: none"> <li>Security Platform</li> </ul>

<a href="#">Security Platform</a>	<ul style="list-style-type: none"><li>• Infineon Security Platform</li></ul>
<a href="#">Security Platform</a>	<ul style="list-style-type: none"><li>• Trusted Platform Module</li></ul>
<a href="#">Security Platform</a>	<ul style="list-style-type: none"><li>• Trusted Computing Group (TCG)</li></ul>



©Infineon

Technologies AG

# **Infineon Security Platform**

# Security Platform

Security Platform Infineon Security Platform





()

Security Platform

: Security Platform () (

)

**Security Platform**

---

---

- 
- 
- 

:

## Security Platform

<b>Windows</b> <b>Windows</b>	<b>Security Platform / Security Platform</b> <b>():</b> Windows () Trusted Platform Module
<b>Security Platform</b>	Security Platform _____
	<b>PKCS #12 :</b> Security Platform
<b>Security Platform</b> <b>Trusted Platform Module</b>	<b>Security Platform</b> <ul style="list-style-type: none"> <li>• Security Platform Infineon Security Platform</li> <li>• Trusted Platform Module Infineon Security Platform</li> </ul> : Trusted Platform Module : <ul style="list-style-type: none"> <li>• Trusted Platform Module</li> <li>• Trusted Platform Module</li> <li>•</li> </ul>  Infineon Security Platform
	Security Platform <ul style="list-style-type: none"> <li>•</li> <li>•</li> </ul>



# **Infineon Security Platform**

## Security Platform Security Platform

- .
- \_\_\_\_\_
- [Security Platform](#)
- [Security Platform](#) - \_\_\_\_\_
  - \_\_\_\_\_
  - \_\_\_\_\_

		Security Platform
	<ul style="list-style-type: none"> <li>•</li> <li>• PIN ( )</li> </ul>	<ul style="list-style-type: none"> <li>• ( )</li> <li>• (- - ...)</li> </ul>
	<ul style="list-style-type: none"> <li>•</li> <li>• PIN ( )</li> <li>•</li> </ul>	<ul style="list-style-type: none"> <li>• (- - ...)</li> </ul>
	<ul style="list-style-type: none"> <li>•</li> <li>• PIN ( )</li> </ul>	<ul style="list-style-type: none"> <li>• Security Platform ( )</li> <li>• (- - ...)</li> <li>• (- - ...)</li> <li>• (- - ...)</li> <li>• (- - ...)</li> </ul>



—



# Security Platform

Security Platform ()

<input type="checkbox"/>	
<input checked="" type="checkbox"/>	Security Platform
<input type="checkbox"/> ...	Security Platform
<input type="checkbox"/>	
<input type="checkbox"/>	
<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/>	Security Platform
<input type="checkbox"/> ...	Security Platform
<b>USB</b>	
<input type="checkbox"/> <i>PIN ()</i>	USB PIN ()
<input type="checkbox"/>	
<input checked="" type="checkbox"/> <i>PIN</i>	Security Platform
<input type="checkbox"/> ...	Security Platform
<input type="checkbox"/>	()


	
<input type="checkbox"/>	
<input checked="" type="checkbox"/>	Security Platform
<input type="checkbox"/> ...	Security Platform



# Security Platform








## Security Platform

0

☒	_____
☒	
<b>USB</b>	
☒	_____
☒	
☒ <i>PIN ()</i>	USB PIN ()
☒	_____
☒	
☒	() 









☒	
☒	_____
☒	

<b>USB</b>	
 PIN ()	USB PIN ()
	_____
	
	_____
	
	() 



( )

	
	
	
	
<b>USB</b>	
 PIN ()	USB PIN ()
	()



©Infineon Technologies AG

# **Infineon Security Platform**

# Security Platform

Infineon Security Platform Security Platform  
 Security Platform



Trusted Computing Management Server

## Security Platform

	...	/
		Security Platform Security Platform  () " (TPM) "
"" " " )	(	Infineon Security Platform Security Platform  "" Security Platform ""
PKCS #12		PKCS #12

- Windows Security Platform  
Windows Windows EFS  
PSD Security Platform

- 
- 
- 
- 
-



:

4 3

- ( **A Z**)
- ( **a z**)
- 10 ( **0 9**)
- (: **!\$#%**)

:

	6

:

	-	-
	6	20

Infineon Security Platform







©Infineon Technologies AG

## **Infineon Security Platform -**

# Infineon Security Platform

Security Platform Trusted Platform Module  
Infineon Security Platform

	<ul style="list-style-type: none"><li>• Infineon Security Platform</li></ul>
<a href="#">_____</a>	<ul style="list-style-type: none"><li>•</li><li>• Security Platform</li><li>• Security Platform</li><li>• Security Platform</li></ul>
<a href="#">_____</a>	<ul style="list-style-type: none"><li>• ()</li><li>•</li><li>•</li></ul> <p> <a href="#">_____</a> Trusted Computing Management Server Personal Secure Drive (PSD)</p>
	<ul style="list-style-type: none"><li>• Security Platform</li><li>• Security Platform</li></ul> <p> Trusted Computing Management Server <a href="#">_____</a></p>
<a href="#">_____</a>	<ul style="list-style-type: none"><li>• ()</li><li>•</li><li>• ()</li><li>•</li></ul> <p> <a href="#">_____</a> Trusted Computing Management Server</p>
<a href="#">BitLocker</a>	<ul style="list-style-type: none"><li>• Trusted Platform Module BitLocker</li></ul> <p> <ul style="list-style-type: none"><li>• BitLocker (: Windows 7</li></ul></p>

Windows Vista Enterprise Ultimate

)

- \_\_\_\_\_ BitLocker  
BitLocker

- 
- Security Platform
- Security Platform /
- Security Platform
- 



- 
- \_\_\_\_\_ Trusted Computing  
Management Server Security Platform

- **Security Platform**

---

 (UAC) (: Windows 7 Windows Vista)

-  **Security Platform**

---

 (UAC) (: Windows 7 Windows Vista)



©Infineon Technologies AG

## **Infineon Security Platform -**



# Infineon Security Platform

Infineon Security Platform

Infineon Security Platform

 <i>Security Platform</i>	Security Platform <a href="#">_____</a>
 <i>Security Platform</i>	<a href="#">Security Platform</a>
 <i>Trusted Platform Module</i>	Trusted Platform Module
	Trusted Platform Module
 ...	Infineon Security Platform



# **Infineon Security Platform -**

:

- 
- 
- 
- 

[Security Platform](#)

:

<input type="checkbox"/> ...	Security Platform (: *.txt)



©Infineon

Technologies AG

**Infineon Security Platform -**

# Security Platform

Infineon Security Platform 4 :

# Trusted Platform Module ()


## Trusted Platform Module

- - Trusted Platform Module Infineon Security Platform
- - Trusted Platform Module BIOS Infineon Security Platform  
: Trusted Platform Module BIOS BIOS Infineon Security Platform Trusted Platform Module
- - Trusted Platform Module  
: Infineon Security Platform Trusted Platform Module

## Infineon Security Platform

- - Infineon Security Platform ( : )  
: [Security Platform](#) \_\_\_\_\_ [Security Platform](#) \_\_\_\_\_  
Security Platform
- - Trusted Platform Module Infineon Security Platform  
Infineon Security Platform Trusted Platform Module
- - Infineon Security Platform Infineon Security Platform  
Security Platform ( 1 )  
: [Security Platform](#) \_\_\_\_\_
- **TPM Security Platform** - Infineon Security Platform  
" OS "  
1 : Windows 7 Windows Vista Trusted Platform  
Module (TPM) Microsoft \_\_\_\_\_  
[\(TPM\)](#) Trusted Platform Module (TPM) Infineon  
Security Platform  
2 : 1

Infineon Security Platform Security Platform ( )  
2)  
: [Security Platform](#) \_\_\_\_\_

- - Infineon Security Platform (:  
)  
: [Security Platform](#) \_\_\_\_\_
- - Infineon Security Platform
- - Infineon Security Platform Infineon Security Platform  
Infineon Security Platform Security  
Platform ( 3)  
:  
[Security Platform](#) \_\_\_\_\_ *Security Platform*  
\_\_\_\_\_ ( \_\_\_\_\_)  
\_\_\_\_\_ **-forceinit** \_\_\_\_\_  
 \_\_\_\_\_ **forceinit**



\_\_\_\_\_


- : / / 2/ :
- /: Trusted Computing Management Server
- /: /-
- /-



# **Infineon Security Platform -**

# Infineon Security Platform

## Infineon Security Platform

 :

- Security Platform
- Infineon Security Platform






Trust Domain

Security Platform

- \_\_\_\_\_

:

- Infineon Security Platform
- \_\_\_\_\_

 ...	
 ...	<ul style="list-style-type: none"> <li>•</li> <li>• (EFS) Personal Secure Drive (PSD)</li> <li>•</li> </ul>
 ...	<p>Security Platform</p> <p><a href="#">Infineon Security Platform</a></p>
 /...	<p>Infineon Security Platform Infineon</p> <p>Security Platform Security Platform EFS</p> <p>Personal Secure Drive Trusted Platform Module</p> <p>Security Platform</p>

Infineon Security Platform



Trusted Platform Module 1.2 Security Platform



©Infineon Technologies AG







## **Infineon Security Platform -**

# Infineon Security Platform

Security Platform Security Platform Personal Secure Drive

 :

- Security Platform

 ...	Security Platform <a href="#">Infineon Security Platform</a>  <ul style="list-style-type: none"><li>• Trusted Computing Management Server</li></ul>
 ...	Security Platform Personal Secure Drive PSD PSD <a href="#">Infineon Security Platform</a>  <ul style="list-style-type: none"><li>• Infineon Security Platform</li><li>• Trusted Computing Management Server</li></ul>
 ...	Security Platform Personal Secure Drive <a href="#">Infineon Security Platform</a>  <ul style="list-style-type: none"><li>• Infineon Security Platform</li><li>• <a href="#">Personal Secure Drive</a> Personal Secure Drive (PSD)</li></ul>

□ ...

Security Platform  
Personal Secure Drive  
PSD PSD

[Infineon Security Platform](#)



- Infineon Security Platform
- \_\_\_\_\_
- \_\_\_\_\_ Personal  
Secure Drive (PSD)

□ ...



©Infineon Technologies AG


# **Infineon Security Platform -**



# Infineon Security Platform

Infineon Security Platform Infineon Security Platform

Infineon Security Platform

	:	<ul style="list-style-type: none"><li>• Security Platform</li><li>• <u>Trusted Computing Management Server</u></li></ul>
---	---	--

 ...	
	Security Platform ... ..
 ...	<u>Infineon Security Platform</u>   <ul style="list-style-type: none"><li>• Infineon Security Platform</li><li>• Infineon Security Platform</li><li>• Infineon Security Platform</li></ul>
 ...	Infineon Security Platform Infineon Security Platform Infineon Security Platform Security Platform   <ul style="list-style-type: none"><li>• Infineon Security Platform</li><li>• Infineon Security Platform</li><li>•</li></ul>

	<p>Security Platform</p> <p style="text-align: center;">...      ...</p>
 	<p style="text-align: right;"><a href="#">Infineon Security Platform</a></p> <hr/>  <ul style="list-style-type: none"> <li>• Infineon Security Platform</li> <li>• Infineon Security Platform</li> </ul>
 ...	<p>Infineon Security Platform Infineon Security Platform XML</p>  <ul style="list-style-type: none"> <li>• Infineon Security Platform ( )</li> <li>• Infineon Security Platform Infineon Security Platform</li> <li>• Infineon Security Platform Infineon Security Platform</li> <li>• Infineon Security Platform</li> </ul>



## **Infineon Security Platform -**

# Infineon Security Platform



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


<input type="checkbox"/> ...	
<input type="checkbox"/> ...	
<input type="checkbox"/> ...	
<input type="checkbox"/> ...	



## **Infineon Security Platform -**




# BitLocker

BitLocker Trusted Platform Module BitLocker  
Microsoft BitLocker

 :

- BitLocker (: Windows 7 Windows Vista Enterprise Ultimate )
- [\\_\\_\\_\\_\\_](#)

## BitLocker

 ...	BitLocker
 ...	Microsoft BitLocker
	 Trusted Platform Module


Technologies AG

## **Infineon Security Platform -**


# Infineon Security Platform

## Security Platform

Infineon Security Platform         Infineon Security Platform

	:	<ul style="list-style-type: none"><li>•</li><li>• <u>                    </u></li> <li>• Windows                                 Windows Home</li><li>• Security Platform</li></ul>
---	---	---

<input type="checkbox"/> ...	Security Platform (
	 <ul style="list-style-type: none"><li>• Infineon Security Platform</li><li>• <u>                    </u> Trust Domain Security Platform</li></ul>

<input type="checkbox"/> ...	<ul style="list-style-type: none"><li>• ()</li><li>•</li><li>•</li><li>•</li></ul> <p><a href="#"><u>Infineon Security Platform</u></a></p>  <ul style="list-style-type: none"><li>• Infineon Security Platform</li><li>• <u>                    </u> Trusted Computing Management Server</li> <li>• <u>                    </u> Infineon Trusted Platform Module</li></ul>
------------------------------	--



## 1.2 Security Platform

☐ ...  
/...

Security Platform /  
Infineon Security Platform

**Security Platform :** Security Platform EFS  
Personal Secure Drive Trusted Platform Module  
Security Platform

Infineon Security Platform

 BitLocker (: Windows Vista Enterprise  
Ultimate) BitLocker Security Platform  
BitLocker

**BIOS Security Platform :** BIOS  
Security Platform Security Platform BIOS  
Security Platform ( [Trusted Platform Module](#)



- Infineon Security Platform BIOS
- Infineon Security Platform
- [Trusted Platform Module /](#)

☐ ...

Security Platform [SpTPMWz.exe](#) -  
*resetattack*



- Trusted Platform Module 1.2 Security Platform
- [Security Platform](#)

☐ ...

Infineon Security Platform [Trusted Computing Management Server](#)



- Windows  
Windows Home
- [Trusted Computing Management Server](#)

□ ...

## Infineon Security Platform \_\_\_\_\_



- Windows Home
- \_\_\_\_\_  
Trusted Computing Management Server



©Infineon Technologies AG

## **Infineon Security Platform -**



:

- 
- \_\_\_\_\_ Trusted Computing Management Server

\_\_\_\_\_

:

<input type="checkbox"/>	
<input type="checkbox"/>	_____
<input type="checkbox"/> ...	
<input type="checkbox"/>	
<input type="checkbox"/>	_____
<input type="checkbox"/>	( )
<input type="checkbox"/> ...	
<input type="checkbox"/> ...	
<input checked="" type="checkbox"/>	



\_\_\_\_\_



## **Infineon Security Platform -**

# Infineon Security Platform

Infineon Security Platform Security Platform

Infineon Security Platform Infineon Security Platform

[Security Platform](#)

[Security Platform](#)



:

- Security Platform
- Security Platform
- 
- ( \_\_\_\_\_ )Security *Mana*
- Platform \_\_\_\_\_ *Management P*
- ( \_\_\_\_\_ )
- Trusted Domain Security Platform

/	
1.	
2.	Security Platform : (EFS)Personal Secure Drive (PSD) (Security Platform )
3. _____	
4.	
5. _____	
6. _____ _____	

Trusted Platform Module ( )

Trusted Platform Module ( )

**Security Platform :**

\_\_\_\_\_

[Security Platform](#)

**Security Platform EFS PSD :**

\_\_\_\_\_

[Security Platform](#)



©Infineon Technologies AG



**Infineon Security Platform -**

\_\_\_\_\_ (: USB )

Security Platform

Security Platform

BitLocker      Personal Secure Drive (PSD) (: USB


)



©Infineon Technologies AG

# **Infineon Security Platform -**

## Security Platform

 :

- *Management Provider*
- Windows Home EFS
- EFS [EFS](#)
- PSD [PSD](#)
- [- - ...](#)

## Security Platform

<input checked="" type="checkbox"/> <i>(EFS)</i>	<p>EFS Microsoft NTFS EFS Security Platform Trusted Platform Module EFS EFS</p> <p>EFS <i>Documents\Encrypted Data My Documents\Encrypted Data ( )</i></p> <p><a href="#"><u>EFS</u></a></p>
<input checked="" type="checkbox"/> <i>Personal Secure Drive (PSD)</i>	<p>PSD PSD PSD PSD PSD PSD</p> <p>PSD PSD PSD <i>Platform ( _____ Personal Secure Drive )</i></p> <p><a href="#"><u>PSD</u></a></p>
<input type="checkbox"/>	<p>Security Platform _____</p>

## EFS PSD ?

### EFS PSD 2

	EFS	PSD
	Windows Home Security Platform	Security Platform
	EFS NTFS	()PSD NTFS
	EFS	<ul style="list-style-type: none"> <li>• EFS : EFS</li> <li>• EFS : <a href="#">PSD</a></li> </ul>
	Web NTFS	
		<a href="#">Security Platform</a>
<i>EFS PSD</i>	(: <i>My Document</i> )	<ul style="list-style-type: none"> <li>• Windows Home EFS</li> <li>• <a href="#">Personal Secure Drive</a></li> <li>• FAT32</li> </ul>



## **Infineon Security Platform -**

## Security Platform



Security Platform PSD



©Infineon Technologies AG



# **Infineon Security Platform - Security Platform**

...



( USB )




---

Technologies AG



©Infineon

## **Infineon Security Platform -**

<input type="checkbox"/> ...	
<input type="checkbox"/> ...	 ( <i>SpProtocol_&lt;PCName&gt;_&lt;UserName&gt;.txt</i> ) ( <i>SpProtocol_&lt;PCName&gt;_&lt;UserName&gt;.</i> <i>&lt;DomainName&gt;.txt</i> )
<input type="checkbox"/>	 (: USB )
	(USB )

# **Infineon Security Platform - Security Platform**



( USB )

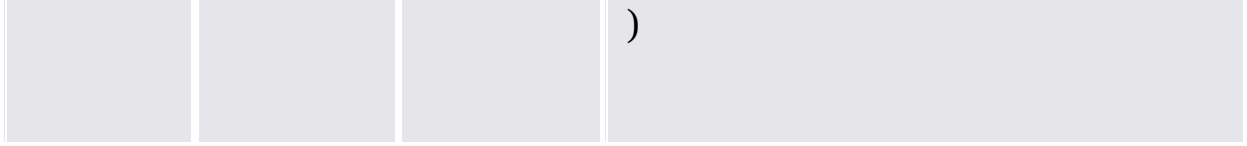
(: USB )

(HD)

USB

HD

(USB HD)	Security Platform		(USB) : SpOwner_<PC>.tpm <PC> ( USB )
/ (HD)	/	( USB )  Platform	/ (USB HD) : SpToken_<PC>.xml <PC> ( USB )
(USB HD)			(USB) : SpPwdResetSecret_<PC>_<User>.xml <PC> , <User> ( ) ( ) ( USB



:



©Infineon Technologies AG



## **Infineon Security Platform -**

# Infineon Security Platform

Infineon Security Platform Security Platform Security Platform (BitLocker) Infineon Security Platform Infineon Security Platform Security Platform \_\_\_\_\_


Security Platform *Security Platform*  
Security Platform

Infineon Security Platform



:

- 
- *Management Provider*  
( \_\_\_\_\_ ) Sec
- Security Platform Security Platform ( \_\_\_\_\_ )
- Trust Domain Security Platform \_\_\_\_\_

1. <a href="#">Trusted Platform Module</a>	Trusted Platform Module
2. ____	Security Platform
3. ____	Security Platform Security Platform
4. .	
5. _____	
6. .	
7. _____	
8. <a href="#">BitLocker</a>	<p><i>BitLocker</i> <i>BitLocker</i></p> <p> <ul style="list-style-type: none"> <li>• BitLocker ( : Windows 7 Windows Vista Enterprise Ultimate )</li> <li>• _____ BitLocker BitLocker</li> </ul> </p>
9. .	Security Platform
10. .	Infineon Trusted Platform Module 1.2 Security Platform

**Security Platform :** \_\_\_\_\_ **Security Platform**  
\_\_\_\_\_ Security Platform

**Security Platform :** Security Platform

- Security Platform () :

... \_\_\_\_\_

- : \_\_\_\_\_ - - ...

- : \_\_\_\_\_ - - ...



©Infineon Technologies AG

## **Infineon Security Platform -**

# Trusted Platform Module

Trusted Platform Module Security Platform Trusted  
 Platform Module Trusted Platform Module Security Platform  
 BIOS


**Physical Presence Interface (PPI) Trusted Platform Module 1.2**  
 Trusted Platform Module BIOS

BIOS

:

Trusted Platform Module

Security Platform Trusted Platform Module

Security Platform		
<b>Trusted Platform Module 1.2 PPI</b>	<input type="checkbox"/>	Trusted Platform Module
<b>Trusted Platform Module 1.2 PPI</b>	<input type="checkbox"/>	Trusted Platform Module
<b>Trusted Platform Module 1.2 PPI</b>	<input type="checkbox"/>	Trusted Platform Module <i>Physical Presence Interface</i>  Trusted Platform Module
(: Trusted Platform	<input type="checkbox"/>	BIOS Trusted Platform

Module 1.1 PPI  
)

Module



:



---




©Infineon Technologies AG

## **Infineon Security Platform -**



# Security Platform

## Security Platform


	Trust Domain Security Platform
 <i>Security Platform</i>	Security Platform
 <i>Security Platform</i>	Trusted Platform Module Security Platform Security Platform Security Platform


## **Infineon Security Platform -**




# Security Platform

Trusted Platform Module () Infineon Security Platform  
Platform Trusted Platform Module Infineon Security Platform

Security Platform

 \_\_\_\_\_ Trust Domain Security Platform

 Security Platform Storage Root Key (SRK)  
Trusted Platform Module 1 Security Platform  
Trusted Platform Module SRK SRK

<input type="checkbox"/>	 _____
<input type="checkbox"/>	()
<input type="checkbox"/>	 _____
<input type="checkbox"/>	
<input type="checkbox"/> ...	
<input checked="" type="checkbox"/>	

 \_\_\_\_\_

**Infineon Security Platform -**

Security Platform \_\_\_\_\_

Security Platform Security Platform \_\_\_\_\_

:

- Microsoft (TPM) \_\_\_\_\_
- Security Platform
- Security Platform OS
- Security Platform OS BIOS Security Platform OS



Trust Domain Security Platform \_\_\_\_\_




©Infineon

Technologies AG






## **Infineon Security Platform -**

# Security Platform

## Security Platform

	<p>Security Platform Trusted Computing Management Server</p> <p style="text-align: right;"><i>BitLocker</i></p>
---	---

## Security Platform

<input checked="" type="checkbox"/> 0	<p>Security Platform</p> 
<input checked="" type="checkbox"/>	 1
<input checked="" type="checkbox"/> <i>BitLocker</i>	<p>Trusted Platform Module BitLocker</p>  BitLocker (: Windows 7 Windows Vista Enterprise Ultimate )
<input checked="" type="checkbox"/>	 1 Security Platform
<input checked="" type="checkbox"/>	 Infineon Trusted Platform Module 1.2 Security Platform

Sec




©Infineon Technologies AG








## **Infineon Security Platform -**

# Security Platform

[Security](#)

	Trusted Computing Management Server
---	--

  ...	Security Platform XML SPSystemBackup.xmlSPSystemBackup  *.xml
 ...	 PC "" " "



## **Infineon Security Platform -**

## Security Platform



- Security Platform
- \_\_\_\_\_/Trusted Computing Management Server



	<ul style="list-style-type: none"><li>•</li><li>•</li></ul> 1
 	XML :
	CD



## **Infineon Security Platform -**



- 
- Trusted Computing Management Server \_\_\_\_\_



	<ul style="list-style-type: none"><li>•</li><li>•</li></ul> 1
abc ...	XML :
	CD





## **Infineon Security Platform -**

# BitLocker

BitLocker Trusted Platform Module



:

- BitLocker (: Windows 7 Windows Vista Enterprise Ultimate )
- BitLocker
- BitLocker BitLocker
- ---



Microsoft BitLocker



©Infineon

Technologies AG

## **Infineon Security Platform -**



:

- 1
- Trusted Computing Management Server



Security Platform



- Security Platform
- 



# **Infineon Security Platform -**

# Infineon Security Platform

Infineon Security Platform Security Platform  
(EFS PSD)

Infineon Security Platform ( Infineon Securiry Platform  
)  
Security Platform \_\_\_\_\_



- *Management Provider*
- (
- ( \_\_\_\_\_ )
- \_\_\_\_\_

(: Security Platform )

1. .	Security Platform 1 Security Platform <a href="#">Platform</a>  Security Platform
2. _____	Security Platform
3. _____	Security Platform
4. <a href="#">Security Platform</a> _____	EFS PSD
5. .	(EFS PSD)
6. ____	
7. .	(EFS PSD)
8. <a href="#">Personal Secure Drive</a>	<i>Personal Secure Drive</i>





: \_\_\_\_\_ Security Platform \_\_\_\_\_  
\_\_\_\_\_ Security Platform

:

- Security Platform (EFS PSD)  
): \_\_\_\_\_  
\_\_\_\_\_

- : \_\_\_\_\_
- : \_\_\_\_\_

: Windows Security Platform  
*SpUserWz.exe* :

<i>-forceinit</i> <i>/forceinit</i>	  _____ <ul style="list-style-type: none"><li>•</li><li>• Trust Domain</li></ul>





## **Infineon Security Platform -**



:


1



## **Infineon Security Platform -**

## Security Platform

 :

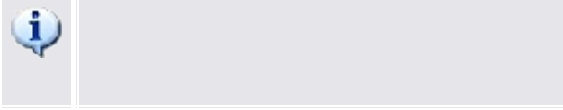
- 
- Security Platform

 <i>Security Platform</i>	Security Platform  _____
 <i>Security Platform</i>	Security Platform  Security Platform Security Platform

---

## **Infineon Security Platform -**

(:)



<input checked="" type="checkbox"/>	A blue information icon (a lowercase 'i' in a circle) is centered in the cell. A thin blue horizontal line is visible on the right side of the cell.
abc <input type="checkbox"/> ...	A blue information icon (a lowercase 'i' in a circle) is centered in the cell.



**Infineon Security Platform -**



( 1 )

:

:

---

Technologies AG




©Infineon




## **Infineon Security Platform -**

# Security Platform

Security Platform ()

	:	1
	:	_____

## Security Platform

<input checked="" type="checkbox"/>	( _____ )
<input checked="" type="checkbox"/>	-  EFS PSD EFS PSD
<input checked="" type="checkbox"/> - <i>EFS</i>	<a href="#">Microsoft</a> <a href="#">(EFS)</a> EFS EFS EFS  Windows Home EFS
<input checked="" type="checkbox"/> - <i>Personal Secure Drive PSD</i>	<a href="#">Personal Secure Drive</a> EFS EFS PSD Security Platform PSD UNC  Personal Secure Drive
<input checked="" type="checkbox"/>	 1

: :


- - EFS PSD
- EFS PSD PSD  
PSD
- EFS PSD EFS PSD PSD -  
(EFS)
- PSD (: PSD )
- Security Platform



©Infineon Technologies AG

## **Infineon Security Platform -**

Infineon Security Platform Infineon  
Security Platform

 : 1 ( [URL](#) )

...

Infineon Security Platform Infineon Security  
Platform



**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 -**



## **Infineon Security Platform -**

# (EFS)

EFS Security Platform Microsoft EFS

<input checked="" type="checkbox"/> EFS	Documents\ My Documents\ ( )  (: EFS desktop.ini FAT32 )
<input checked="" type="checkbox"/>	EFS  ( )
<input type="checkbox"/> ...	Security Platform EFS (Microsoft EFS)  Microsoft EFS : <ul style="list-style-type: none"><li>• EFS EFS Security Platform EFS Microsoft EFS</li><li>• (Security Platform ) Microsoft EFS</li></ul> : EFS EFS  EFS

# **Infineon Security Platform**

# Personal Secure Drive

Personal Secure Drive Personal Secure Drive

Personal Secure Drive Personal Secure Drive

           *Personal Secure Drive (PSD)*

## Personal Secure Drive

	/
PSD	1. <a href="#">Personal Secure Drive</a> 2. <a href="#">Personal Secure Drive</a>
PSD	1. <a href="#">Personal Secure Drive</a> 2. <a href="#">Personal Secure Drive</a>
PSD	1. <a href="#">Personal Secure Drive</a> ( 1 PSD ) 2. <a href="#">Personal Secure Drive</a> 3. <a href="#">Personal Secure Drive</a>







# **Infineon Security Platform**

# Personal Secure Drive

Personal Secure Drive PSD

 <i>Personal Secure Drive</i>	Personal Secure Drive ( <a href="#">Drive</a> )
 <i>Personal Secure Drive</i>	32
<input checked="" type="checkbox"/> <i>Personal Secure Drive</i>	PSD
<input checked="" type="checkbox"/>	PSD







# **Infineon Security Platform**

# Personal Secure Drive

Personal Secure Drive 1

Personal Secure Drive

	<p>(MB) (: USB )</p> <p>Personal Secure Drive Personal Secure Drive</p> <p> _____ PSD</p> <p>PSD ( <a href="#">Personal Secure</a></p> <p>PSD</p>
 PSD	<p> _____ <i>Personal Secure Drive</i></p>

# PSD

Personal Secure Drive

PSD PSD

PSD :

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

[PSD](#)







©Infineon Technologies AG

# **Infineon Security Platform**

# Personal Secure Drive

Personal Secure Drive Personal Secure Drive  
Personal Secure Drive  
1 Personal Secure Drive Personal Secure Drive

*Personal Secure Dr*

 <b>Personal Secure Drive</b>	<b>Personal Secure Drive "F5"</b> <b>Personal Secure Drive Personal Secure Drive</b>
 PSD	<b>Personal Secure Drive (: PSD )</b> <a href="#"><u>Personal Secure Drive</u></a>
 PSD	<b>Personal Secure Drive</b> <a href="#"><u>Personal Secure Drive</u></a>
 PSD	<b>Personal Secure Drive</b> <a href="#"><u>Personal Secure Drive</u></a>




# **Infineon Security Platform**



# Personal Secure Drive

## Personal Secure Drive PSD

<input checked="" type="checkbox"/> <i>Personal Secure Drive</i>	Personal Secure Drive ( <a href="#">Drive</a> )
<input type="checkbox"/> <i>Personal Secure Drive</i>	
<input checked="" type="checkbox"/> <i>Personal Secure Drive</i>	PSD
<input checked="" type="checkbox"/>	PSD  0



©Infineon

**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*

---

Technologies AG



©Infineon

# **Infineon Security Platform -**

# Infineon Security Platform

Infineon Security Platform Infineon Security Platform  
Infineon Security Platform Infineon Security Platform

Infineon Security Platform Infineon  
Security Platform

Infineon Security Platform Infineon Security Platform  
Infineon Security Platform

Infineon Security Platform Infineon Security Platform

Infineon Security Platform ()



:

- . Security Platform
- Infineon Security Platform  
Security Platform Trusted Computing  
Management Server

1. _____	Security Platform Security Platform
2. _____	(            )
3. _____	
4. _____	

:  
- - ... - -  
...

## **Infineon Security Platform -**



Security Platform Security Platform



Trusted Computing Management Server

⊙	Infineon Security Platform Infineon Security Platform
⊙	Infineon Security Platform Infineon Security Platform Infineon Security Platform



©Infineon

Technologies AG

## **Infineon Security Platform -**



## Trusted Computing Management Server

abc

...



XML



©Infineon Technologies AG

## **Infineon Security Platform -**



## Trusted Computing Management Server

abc

...



XML



©Infineon Technologies AG

## **Infineon Security Platform -**

Infineon Security Platform Infineon Security Platform  
Infineon Security Platform



Trusted Computing Management Server



Security Platform

Infineon Security Platform  
Infineon Security Platform systems 1



Infineon Security Platform  
Infineon Security Platform Infineon  
Security Platform [Infineon Security Platform](#)



©Infineon

Technologies AG

## **Infineon Security Platform -**



# Infineon Security Platform

Infineon Security Platform

[Security Platform](#)

(" ID")

(" ID")



Security Platform



[Trusted Computing Management Server](#)  
Personal Secure Drive (PSD) Personal Secure Drive



[\(UAC\)](#) (: Windows 7  
Windows Vista)

	<a href="#">_____</a>	
	<a href="#">PSD_____</a>	Personal Secure Drive
		Personal Secure Drive
	<a href="#">_____</a>	Personal Secure Drive
	<a href="#">_____</a>	Personal Secure Drive
	<a href="#">_____</a>	Personal Secure Drive
	<a href="#">_____</a>	Personal Secure Drive
	<a href="#">PSD</a>	Personal Secure Drive

Security Platform







: : - - \_\_\_\_\_

: : \_\_\_\_\_ - - .

**():** Security Platform Security  
Platform Security Platform

: Security Platform \_\_\_\_\_  
(: Security Platform )

## **Infineon Security Platform -**

	<p>Infineon Security Platform ( )</p> <p> _____ Personal Secure Drive (PSD)</p>
	<p>Infineon Security Platform</p> <p> _____ Personal Secure Drive (PSD)</p>
	<p>Infineon Security Platform</p> <p> <ul style="list-style-type: none"> <li>• _____ Trusted</li> <li>• _____ Computing Management Server</li> </ul> </p>



## **Infineon Security Platform -**



Trusted Computing Management Server

abc

...

Security Platform



XML







© Infineon Technologies AG

# **Infineon Security Platform -**



# Personal Secure Drive

Personal Secure Drive PSD PSD

 <i>Personal Secure Drive</i> ...	1 Personal Secure Drive  Personal Secure Drive
 <i>Personal Secure Drive</i>	Personal Secure Drive Personal Secure Drive  Personal Secure Drive Personal Secure Drive  :
 ...	/   *.fsb



## **Infineon Security Platform -**



: \_\_\_\_\_ Trusted Computing  
Management Server



*Trusted  
Platform Module  
Security  
Platform*

Security Platform 1

- : Security Platform  
Security Platform
- *Trusted Platform Module* : Security Platform  
Security Platform  
Security Platform  
Trusted Platform Module BIOS
- *Security Platform* : Security Platform  
Security Platform  
Security Platform PC



abc

...



XML



## **Infineon Security Platform -**

# Personal Secure Drive

Personal Secure Drive PSD PSD

<p>abc <i>Personal Secure Drive</i> ... ...</p>	<p>1 Personal Secure Drive PSD ... Personal Secure Drive PSD</p>
<p><input type="checkbox"/> <i>Personal Secure Drive</i></p>	<p>Personal Secure Drive Personal Secure Drive : • Personal Secure Drive (PSD ) PSD • Personal Secure Drive ( PSD )PSD • Personal Secure Drive Personal Secure Drive :</p>
<p><input type="checkbox"/> ...</p>	<p>Personal Secure Drive Personal Secure Drive PSD</p>
<p><input type="checkbox"/> ...</p>	<p>Personal Secure Drive : • PSD • PSD</p>

- PSD

PSD








© Infineon Technologies AG

## **Infineon Security Platform -**

# / Personal Secure Drive

Personal Secure Drive Personal Secure Drive

:

 		PSD	
	PSD	>	
	Personal Secure Drive ( <a href="#">Personal Secure Drive</a> )		
	32 "My Secure Drive"		
<input checked="" type="checkbox"/>	PSD		
<input checked="" type="checkbox"/>	PSD		





## **Infineon Security Platform -**



:

- 
- Trusted Computing Management Server

abc: /  
ID

ID  
 ID

abc  
:/  
ID

ID

## **Infineon Security Platform -**



:

- 
- Trusted Computing Management Server

abc: /  
ID

ID  
 ID


: /  
ID

ID  
1





## **Infineon Security Platform -**

## Security Platform

 :

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

abc ... 	 XML
xxx	

## **Infineon Security Platform -**



:

- 
- Trusted Computing Management Server

abc :  
/ ID

ID  
 ID

abc  
: /  
ID

ID



© Infineon



## **Infineon Security Platform -**



:

- 
- Trusted Computing Management Server

abc ▼	
abc ▼	<>  



## **Infineon Security Platform -**

# Infineon Security Platform

Infineon Security Platform




:

- \_\_\_\_\_ Security Platform
- \_\_\_\_\_ Trusted Computing Management Server



\_\_\_\_\_(UAC)\_\_\_\_\_ (: Windows 7  
Windows Vista)

: Security Platform


1. _____	
2. _____	
3. _____	()
4. _____	
5. _____	 _____

Infineon Security Platform :



© Infineon Technologies AG

## **Infineon Security Platform -**

1	 Trusted Computing Management Server
( )	

 Security Platform

---

 © Infineon Technologies AG



## **Infineon Security Platform -**



Trusted Computing Management Server

\_\_\_\_\_



Security  
Platform ( \_\_\_\_\_ )



© Infineon Technologies AG

## **Infineon Security Platform -**



:

Trusted Computing Management Server

abc	(
...	
xxx	: " " " " ""



## **Infineon Security Platform -**



:



Trusted Computing Management Server

abc	
...	00
abc	



## **Infineon Security Platform -**

: "" "

abc	( _____ )
<input type="checkbox"/> ...	
<input checked="" type="checkbox"/>	 _____
	:
abc	Security Platform
<input type="checkbox"/> ...	
<input type="checkbox"/> ...	_____  Trust Domain
abc	





## **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 :** PKCS #12 *Microsoft*

**Security Platform PC :** PKCS #12 *Security Platform*  
*PKCS #12* Trusted Platform Module

1. <a href="#">PKCS #12</a>	
2. <a href="#">___</a>	PKCS #12

Infineon Security Platform PKCS #12 Security  
Platform ... Security Platform  
(     - - ...     )



©Infineon

---

Technologies AG

## **Infineon Security Platform - PKCS #12**

# PKCS #12

PKCS #12

abc	D:\certificates\MyPKCS12file.pfx D:\certificates\MyPKCS12file.p12
	PKCS #12
xxx	PKCS #12





©Infineon Technologies AG

## **Infineon Security Platform - PKCS #12**



# PKCS #12

<input type="checkbox"/>	PKCS #12
<input type="checkbox"/> ...	 CA :
<input checked="" type="checkbox"/> PKCS #12	PKCS #12 (CA) ( PKCS #12 )   CA : CA CA PKCS #12  → → CA → CA
<input checked="" type="checkbox"/>	



# **Infineon Security Platform -**

# Security Platform

Security Platform

	<p>(TNA) Security Platform</p> <p>Security Platform :</p> <p> Security Platform</p> <p>Security Platform Security Platform</p> <p> Security Platform</p> <p> Security Platform</p> <p>Security Platform Security Platform</p> <p> Security Platform</p> <p> Security Platform</p>
	<p>:</p> <ul style="list-style-type: none"><li>• Security Platform</li><li>• Security Platform</li><li>• Security Platform</li><li>•</li></ul> <p> _____</p>
	<p>Security Platform Security Platform</p> <p> _____ Trusted Computing Management Server</p>

---




©Infineon Technologies AG

## **Infineon Security Platform -**

# Infineon Security Platform

## Infineon Security Platform

 [\(UAC\)](#) (: Windows 7  
Windows Vista)

<i>Security Platform</i>	<a href="#">Infineon Security Platform</a>  (UAC)
<i>Security Platform</i>	<a href="#">Infineon Security Platform</a> Infineon Security Platform (Security Platform )  _____ Trust Domain Security Platform
<i>Security Platform</i>	<a href="#">Infineon Security Platform</a> Infineon Security Platform Security Platform ( )  _____
<i>Security Platform</i>	Security Platform _____ Security Platform  _____ Trusted Computing Management Server
	Security Platform _____
<i>Personal</i>	Personal Secure Drive _____ PSD ( <:

<p><i>Secure Drive -</i></p> <p><i>Personal Secure Drive -</i></p> <p>&lt;: &gt; -</p>	<p>&gt; )</p> <p>PSD</p>
<p><i>Personal Secure Drive -</i></p> <p><i>Personal Secure Drive -</i></p> <p>&lt;: &gt; -</p>	<p>Personal Secure Drive ___ PSD ( &lt;:</p> <p>&gt; )</p> <p>PSD</p>
<p><i>Personal Secure Drive -</i></p> <p><i>Personal Secure Drive -</i></p> <p>&lt;: &gt; -</p>	<p>Windows PSD PSD ( &lt;:</p> <p>&gt;)PSD</p> <p>1 PSD</p>
<p><i>Personal Secure Drive -</i></p> <p>/</p>	<p>Personal Secure Drive _____</p>
<p><i>Personal Secure Drive -</i></p>	<p>Personal Secure Drive _____</p>
<p><i>(EFS)</i></p>	<p>(Encrypting File System) EFS</p> <p>EFS</p>
	<p>_____</p>

	<p>Security Platform Security Platform</p> <ul style="list-style-type: none"> <li>• _____</li> <li>• Security Platform Security Platform</li> </ul>
	<p>Security Platform PSD EFS :</p> <ul style="list-style-type: none"> <li>• EFS PSD EFS PSD PSD (EFS)</li> <li>• PSD (:)</li> </ul>
<i>Security Platform</i>	<p>Infineon Security Platform Security Platform EFS Personal Secure Drive Trusted Platform Module Security Platform Infineon Security Platform Infineon Trusted Platform Module 1.2 Security Platform</p>
<i>Security Platform</i>	<p>Security Platform Security Platform Security Platform 1.2 Trusted Platform Module Security Platform Security Platform</p> <p> _____ Trust Domain Security Platform</p>
<i>Security Platform</i>	<p>Security Platform Security Platform Platform</p> <p> _____ Trusted Computing Management Server</p>
<i>Security Platform</i>	<p>Security Platform</p> <p> _____ Trusted Computing Management Server</p>



/ -

## Trusted Computing Management Server

(  
/)



## Trusted Computing Management Server

:

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

/ -

## Trusted Computing Management Server



:

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



:

- 
- Security Platform Trusted Computing Management Server

	
<i>Infineon TPM Strong Cryptographic Provider</i>	<a href="#"><u>Infineon TPM Strong Cryptographic Provider</u></a>
	Infineon Security Platform
	Platform



**Infineon Security Platform -**

# Infineon Security Platform

Trusted Platform Module 2

- 

Infineon Trusted Platform

- 

Infineon Security Platform  
Platform

[Infineon Security](#)

Infineon Security Platform Infineon Security Platform  
BIOS



©Infineon

---

Technologies AG

**Infineon Security Platform -**

# Infineon Security Platform

Infineon Security Platform Infineon Security Platform  
Infineon Security Platform

Infineon Security Platform

Trusted Platform Module



©Infineon

---

Technologies AG



**Infineon Security Platform**

# Infineon Security Platform

Security Platform **<b></b>** **<b>...</b>** ( ): [Security Platform](#)

Security Platform \_\_\_\_\_  
\_\_\_\_\_ Security Platform



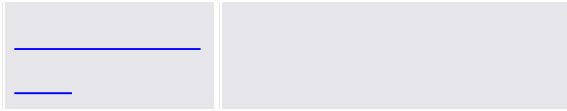
©Infineon

Technologies AG

# **Infineon Security Platform -**

# Infineon Security Platform

Infineon Security Platform



\_\_\_\_\_ Trusted Computing Management Server



- 
- Windows Home

# Security Platform

ADMX (Windows 7 Windows Vista) Security Platform

(

Security Platform (  
**IfxSpPol.adm**):

1. (gpedit.msc)

2.

3. ...

""

4.

" "

5. **IfxSpPol.adm** "Security Platform"

6.

1. \_\_\_\_\_  
(UAC) ( Windows 7 Windows Vista)

 **Security Platform**

**Security Platform**

2. \_\_\_\_\_

...

Infineon Security Platform

Microsoft Microsoft TechNet  
Microsoft Windows F1



©Infineon Technologies AG



## **Infineon Security Platform -**

# Infineon Security Platform



Infineon Security Platform





Trusted Computing Management  
Server Trusted Computing Management Server



: ( ) Security Platform

<i>TPM</i>	<ul style="list-style-type: none"> <li>: Trusted Platform Module Physical Presence Interface (PPM)</li> <li>Trusted Platform Module</li> <li>: Trusted Platform Module</li> </ul>	
	<ul style="list-style-type: none"> <li>:</li> <li>: Trusted Computing Group (TCG) Security Platform</li> <li>Trusted Domain</li> <li> Security Platform</li> </ul>	
<i>TPM NV</i>	<ul style="list-style-type: none"> <li>Trusted Platform Module 1.2 (NV)</li> <li>:</li> <li>NV</li> <li>: NV</li> <li> Trusted Platform Module 1.2</li> <li>Security Platform</li> <li>Security Platform</li> </ul>	/ NV
	<ul style="list-style-type: none"> <li>TPM</li> <li>: (: Security Platform )</li> <li>: PIN Windows BitLocker )</li> <li>:</li> </ul>	<ul style="list-style-type: none"> <li>: 3</li> <li>: 5</li> <li>: 10</li> </ul>

	 Infineon Trusted Platform Module 1.2 Security Platform Security Platform ( Security Platform )	
	: ( : ) : ( : )	
	: (S3) (S4) Security Platform Security Platform : Security Platform	
	: ID (CLSID) CLSID ID ID: {76D8D888-B5AC-49FC-9408-8A45D37F3AC6} :	
	: :  Trusted Domain	
<i>SRK</i>	Trusted Platform Module Storage Root Key (SRK) SRK Security	

Platform SRK

: SRK

: SRK SRK



Trusted Domain



:

: Security Platform



: Security Platform

: :

\\ServerName\FolderName\ArchiveName.xml

Security Platform PC PC



Security Platform PC

:

: Security

Platform

Security Platform

: Security Platform

- ...

: :

\\ServerName\FolderName\ArchiveName.xml

Security Platform PC PC



Security Platform PC

:

\_\_\_\_\_

\_\_\_\_\_

	Security Platform	---
	Security Platform	
<i>URL</i>	<a href="#">_____</a>	





## **Infineon Security Platform -**

# Infineon Security Platform



Infineon Security Platform



Trusted Computing Management  
Server Trusted Computing Management Server



: ( ) Security Platform

-	: :6 : 6 <hr/>	6
-	: : <hr/>	
-	( ) : • : 42 • : 7 : 	
-	: : 20 : 20 	20
-	: : 	

	/: Security Platform	

/: EFS PSD

:

/ *Security Platform* : Infineon Security Platform  
Security Platform

: Security Platform Infineon  
Security Platform



Security Platform Infineon Trusted Module 1.1  
Security Platform

: Security Platform

:

*EFS* : Security Platform (*EFS*)

:



Windows Home EFS

*PSD* : Security Platform *Personal Secure Drive (PSD)*

:

: Security Platform ( )

: Security Platform ( ) ( )



1 Security Platform

: Infineon Security Platform

:

:  
Security Platform

:

...

URL : [Infineon Security Platform](#)

1

: Infineon Security Platform

:

- Security Platform
- :
- EFS ( EFS )

EFS : EFS CA () EFS

**1. EFS : ()**

- : CA ()
- : WWW CA
- : PC

**2. URL: EFS CA**

https://www.companyname.com/foldername

EFS CA

- URL
- EFS
- EFS Security Platform PC EFS

: EFS EFS EFS

:

- EFS EFS PSD
- (EFS PSD) EFS ( URL )

**EFS**

EFS : Security Platform EFS : 14

:

14

EFS : EFS

: 10

10 Personal Secure Drive /PSD : Personal Secure Drive  
(: C:) Personal Secure Drive

: Personal Secure Drive

PSD : PSD ( ) PSD PSD

: PSD

:\_

5000MB

Windows 7 Windows Vista PSD 20MB PSD  
10MB

- PSD 5050MB PSD 50MB
- 5000MB PSD

5000MB : Security Platform Security Platform

: Security Platform Security Platform

MS-CAPI

: MS-CAPI ""

:



/: Infineon TPM Strong Cryptographic Provider  
Infineon TPM Strong Cryptographic Provider  
\n\n/:

: Infineon TPM Strong Cryptographic Provider

/

	: Security Platform () : 2 :	
	/ <b>Management Provider</b> : Management Provider  / <b>Management Provider</b> : Management Provider  :	/ <b>Management  Provider</b>



# **Infineon Security Platform**



# Security Platform

Security Platform Trusted Platform Module Microsoft  
 Crypto-API Microsoft Cryptography Next Generation (CNG) API PKCS #11  
 Crypto-API

Provider		Crypto-API	/ ()
Infineon TPM Cryptographic Provider ( CSPAES )	<hr/> Trusted Platform Module	Microsoft Crypto-API	<ul style="list-style-type: none"> <li>• EFS PSD</li> <li>• Outlook Windows Mail/Outlook Express (S/MIME)</li> <li>• Internet Explorer SSL/TLS</li> <li>• Internet Explorer</li> <li>• Microsoft (CA)</li> <li>• Microsoft Office</li> <li>• Microsoft Crypto-API Checkpoint VPN</li> <li>• Microsoft Crypto-API Entrust</li> <li>• Adobe Adobe</li> <li>• EAP-TLS</li> </ul>
Infineon TPM RSA and AES Cryptographic Provider ( CSPAES Windows 2000 )			

<p>Infineon TPM PKCS #11 Provider ("TPM Cryptoki Token" )</p>		<p>PKCS #11 Crypto-API</p>	<ul style="list-style-type: none"> <li>• Mozilla Thunderbird (S/MIME)</li> <li>• Mozilla Firefox SSL/TLS</li> <li>• Mozilla Firefox (CA)</li> <li>• Sun Certificate Server CA</li> <li>• RSA SecurID Web</li> <li>• PKCS #11 Entrust</li> </ul>
<p>Infineon TPM Strong Cryptographic Provider (AES )</p>	<p>Trusted Platform Module</p>	<p>Microsoft <u>Crypto-API</u></p>	<ul style="list-style-type: none"> <li>• VPN</li> </ul>
<p>Infineon TPM Platform Cryptographic Provider ( CSP)</p>	<p>Trusted Platform Module  Trusted Platform Module Platform CSP</p>	<p>Microsoft Crypto-API</p>	<ul style="list-style-type: none"> <li>• LAN RADIUS (TLS ) IEEE 802.1X EAP-TLS</li> <li>• LAN RADIUS (TLS</li> </ul>

			<ul style="list-style-type: none"> <li>) IEEE 802.1X EAP-TLS</li> <li>• VPN IPSec</li> </ul>
Infineon TPM Key Storage Provider (KSP)	Infineon TPM Cryptographic Service Provider TPM RSA	Microsoft Cryptography Next Generation (CNG) API	<ul style="list-style-type: none"> <li>• Microsoft .NET 3.0</li> <li>• Cryptographic Service Provider</li> </ul>



# **Infineon Security Platform**

# Security Platform

Security Platform Trusted Computing Group (TCG)

TCG (TSS)

- TSS (TCG )

- TSS

- TSS

TCG TCG



Trusted Platform Module



---

©Infineon Technologies AG

# **Infineon Security Platform**

# Server

Server Trusted Computing Management Server Server  
Security Platform ( \_\_\_\_\_ )

(GUI) Server Client  
Side Control Agent

<i>Client Side Control Agent</i>	Client Side Control Agent Trusted Computing Management Server ( _____ )

Infineon TPM Professional Package Software Server

Server \_\_\_\_\_ *Client Side Control Agent* *ReadmeServerIntegrationService.*



©Infineon Technologies AG

# **Infineon Security Platform**



# Security Platform

Infineon Security Platform  
[PKCS #11 PKI](#)

[Windows 2000/Windows XP](#)  
Infineon Security Platform

- [Personal Secure Drive \(PSD\)](#)
- [\(EFS\)](#)
- [\\_\\_\\_\\_\\_](#)
- [Microsoft Word](#)
- [\\_\\_\\_\\_\\_](#)



©Infineon

---

Technologies AG

# **Infineon Security Platform**

(PKI)

Security Platform 1 (CA) (PKI)

[Security Platform](#)



(PKI)

[Windows \(PKI\)](#)

[PKCS #11 \(PKI\)](#)

---

Technologies AG



©Infineon

**Infineon Security Platform**

()

- 
- 
- 
- 
- (CA)
- (CA)

- 
- ()
- ()

(CA: Certificate Authority)

---

Technologies AG



# **Infineon Security Platform**

# CA

Microsoft            **ID**    ID VeriSign Thawte (CA)

CA

- 
- 
- 

CA CA CA Certificate Practices Statement (CPS)  
CA CA Web CPS

CA

- CA ?
- CA ? CA CA ? CA
- CA ?
- CA ?
- CA ?

CA CA CA



Security Platform

[Cryptographic Service Provider](#) 1



©Infineon

Technologies AG

**Infineon Security Platform**



# Windows (PKI)

Microsoft Windows 2000 Windows (PKI)  
Windows

PKI (DC) Kerberos (KDC) Windows  
PKI (PKI)  
ID  
Windows NT4  
(PKI) (CRL) (CA) (PKI)

Microsoft PKI Microsoft TechNet

PKI ()

- [Active Directory](#)
- [\(CA\)](#)
- [\\_\\_\\_\\_\\_](#)
- [.](#)

---

Technologies AG



©Infineon

**Infineon Security Platform**

# Active Directory

Active Directory Microsoft Windows 2000 Windows 2000  
Active Directory ()

CA Active Directory PKI Active Directory

Active Directory  
"Active Directory "

Active Directory Microsoft TechNet

PKI ()

---

Technologies AG



©Infineon

**Infineon Security Platform**

(CA)

(CA) (PKI) CA CA CA  
CA (CA CA)

Windows 2000 (PKI) CA CA

Windows 2000 2 CA 2 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  
[Cryptographic Service Provider](#)



©Infineon

---

Technologies AG

**Infineon Security Platform**

\_\_\_\_\_ Active Directory 1 Cryptographic Service  
Provider (CSP) Security Platform  
[Service Provider](#)

# Active Directory

## 1. ADSI Edit

Active Directory (ADSI )  
Microsoft Windows 2000 Server  
CD Support\Tools  
Windows 2000 Windows 2000 Server  
CD Support\Tools Readme.doc ADSI Edit  
Microsoft Windows 2000

## 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=**

*pKIDefaultCSPs*

:

*<n>, Infineon TPM Cryptographic Provider ( <*

2

*1, Microsoft Enhanced Cryptographic Provider v1.0*

*2, Microsoft Base Cryptographic Provider v1.0*

*3, Infineon TPM Cryptographic Provider*



(CA) [Security Platform](#)

Security Platform  
Active Directory

[Cryptographic Service Provider](#)



©Infineon Technologies AG

**Infineon Security Platform**

Security Platform

[Cryptographic Service Providers](#) 1

- [Microsoft](#)
- [Microsoft Windows Server Web](#)



©Infineon

Technologies AG

**Infineon Security Platform**

# Microsoft

CA Windows

1. Microsoft  
Microsoft

2.

...

3.

4. Security Platform  
[Cryptographic Service Provider](#) 1

5. Security Platform Cryptographic Service Provider 1  
CSP



Security Platform Cryptographic Service Provider

6.

7.

8.




**Infineon Security Platform**

# Web

Microsoft Windows server (: Microsoft Windows Server 2003) Microsoft CA

CA Web

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


 Security Platform  
[Cryptographic Service Provider](#) 1

Cryptographic Service Provider

CSP:	<i>MS Base Cryptographic Provider V1</i>
:	<i>CSP</i>
:	
:	<i>GUID</i>

*MS Base Cryptographic Provider V1*

Security Platform Cryptographic Service Provider 1  
CSP GUID

 Security Platform Cryptographic Service Provider



# **Infineon Security Platform**



## PKCS #11 (PKI)

PKCS #11 : Public Key Cryptography Standards () #11

PKCS #11

(IC )

PKCS #11

PKCS #11

PKCS #11

PKCS #11 PKCS #11 (PKI :

Public Key Infrastructure) PKCS #11

PKCS #11 PKCS #11

LDAP (Lightweight Directory Access Protocol)

Windows 2000 / XP PKCS #11 Security Platform

PKCS #11 () Trusted Platform

Module

PKCS #11 PKCS #11

PKCS #11 PKCS #11

PKCS #11

(PKI) (CRL) (CA) (PKI)

(PKI)

- 
- (CSP)
- Infineon Security Platform PKCS #11
- (CA)

[Mozilla Firefox](#)

(PKI) PKI



Security Platform PKCS#11 DLL  
(*ifxtpmck.dll*) Security Platform  
PKCS#11 Security Platform

*system32*

*ifxtpmck.dll*

---

Technologies AG



**Infineon Security Platform**

# PKCS #11 Mozilla Firefox

PKCS #11 (PKI : Public Key Infrastructure)

PKCS #11 Infineon Security

Platform Infineon Security Platform PKCS #11

() Trusted Platform Module

Mozilla Firefox PKCS #11 PKCS #11

Infineon Security Platform PKCS #11 Mozilla

Firefox PKCS #11 PKCS #11

# Mozilla Firefox

1. Mozilla Firefox

2. > ...

3.

4.

5. 2 **OK**  
Platform

6. **OK**

Mozilla Firefox 

---

## Mozilla Firefox

- 1.
- 2.
- 3.
4. PKCS#11
- 5.
- 6.

*IfxTPMCK.dll* PATH

**OK**



©Infineon

Technologies AG

**Infineon Security Platform**

Security Platform

[Cryptographic Service Providers](#) 1

- [Sun Certificate Server](#)
- [PKCS #11 CA](#)



©Infineon

---

Technologies AG



**Infineon Security Platform**

# Sun Certificate Server CA

Sun Certificate Server CA (Windows 2000 /  
XPUnixLinux )

PKCS #11 Web

# Mozilla Firefox

1. Mozilla Firefox
2. Mozilla Firefox
3. Web  
1025 SSL Web  
*https://your\_server\_name:1025*

4.

5. (CA)

- 
- / **Web**
- 

: Web

(CA)

1. > ...

2. ...

3. CA

- CA Web **Web**
- CA
- CA



**Infineon Security Platform**

PKCS #11 CA

CA Web

: [Sun Certificate Server](#) CA

---

Technologies AG



©Infineon

# **Infineon Security Platform**

# Personal Secure Drive

Personal Secure Drive (PSD) 1  
Personal Secure Drive

Personal Secure Drive Personal Secure  
Drive Personal Secure Drive

Personal Secure Drive 2

- 1.
- 2.

Personal Secure Drive    AES RSA    Personal  
Secure Drive Personal Secure Drive Personal  
Secure Drive Personal Secure Drive Personal Secure  
Drive Personal Secure Drive



PSD

PSD



\_\_\_\_\_ Trusted Computing Management Server PSD PSD  
( \_\_\_\_\_ )



PSD

PSD (: USB ) PSD

(: ) PSD PSD

1 (  
PSD

[Security P](#)



©Infineon Technologies AG

**Infineon Security Platform**

# Personal Secure Drive

Personal Secure Drive

:

- AES (Advanced Encryption Standard)
- RSA
- - /
- -

## Personal Secure Drive :

- : Personal Secure Drive Windows
- 
- Microsoft EFS ( )

# Trusted Platform Module

Personal Secure Drive Trusted Platform Module (TPM) Personal  
Secure Drive Trusted Platform Module  
Trusted Platform Module

# Personal Secure Drive

- 
- Trusted Platform Module (TPM)
- 
- Windows :
- /:
- /:



©Infineon

---

Technologies AG

# **Infineon Security Platform - PSD PSD**

# Personal Secure Drive

Personal Secure Drive () ()

PSD PSD PSD PSD



# PSD

\_\_\_\_\_ PSD ( 1 Personal Secure Drive )

**Personal Secure Drive - ( Personal Secure Drive )**  
**Secure Drive - <: > -**

**Personal**

Windows PSD

# PSD

Windows PSD

         ( 1 Personal Secure Drive )  
**Secure Drive -**  
**Drive - <: > -**

**Personal**  
( Personal Secure Drive )      **Personal**

PSD

         PSD ( 1 Personal Secure Drive )

**Personal Secure Drive -** ( Personal Secure Drive )

**Secure Drive - <: > -**

**Personal**

PSD

PSD Security Platform

# PSD

PSD Personal Secure Drive PSD

<b>PSD</b>	
<input type="checkbox"/> <i>Personal Secure Drive</i>	Personal Secure Drive "F5"
<input checked="" type="checkbox"/>	Personal Secure Drive PSD PSD
<input type="checkbox"/>	
<input type="checkbox"/>	PSD PSD



©Infineon Technologies AG

**Infineon Security Platform**

# Personal Secure Drive

Personal Secure Drive

Personal Secure Drive

[Infineon Security Platform](#)



# Personal Secure Drive

Personal Secure Drive

7 ""

Windows

HKEY\_LOCAL\_MACHINE\Software\Infineon\TPM  
Software\PSD\DLSkip

: 7 9 9 9



©Infineon

---

Technologies AG

# **Infineon Security Platform**

# Personal Secure Drive

Personal Secure Drive PSD PSD

[Windows XP Home](#) Windows

Windows Vista Basic Home Windows Vista Home Premium

Home Home PSD

PSD



## PSD

- 1 PSD
- PSD

PSD

[PSD](#)

# PSD

PSD	EFS Windows	EFS Windows
	<ul style="list-style-type: none"> <li>• PSD PSD</li> <li>PSD</li> <li>• PSD</li> </ul>	<ul style="list-style-type: none"> <li>• EFS</li> <li>• Microsoft</li> <li>• PSD PSD</li> </ul>
<b>PSD</b>	<ol style="list-style-type: none"> <li>1. <a href="#">PSD</a></li> <li>2. PKCS #12 PKCS #12 : PSDRecovery /R:</li> <li>3. PSD : : PSDRecovery /A:.CER [/ID:driveID] : 2 1</li> </ol>	<ol style="list-style-type: none"> <li>1. <a href="#">PSD</a></li> <li>2. Microsoft EFS : : secpol.msc</li> <li>3. <a href="#">PSD</a> : 2 1 3 Windows 2000 EFS Windows 7 Windows VistaWindows XP Professional</li> </ol>
	PSD	Microsoft EFS : : secpol.msc

	: PSDRecovery /V [/ID:driveID]			
	PSD 1 : PSDRecovery /D:[] [/ID:driveID]	Microsoft EFS : : secpol.msc		
<b>PSD</b>	<ul style="list-style-type: none"> <li>• ( PKCS #12 <a href="#">_____</a>)</li> <li>• Personal Secure Drive</li> <li>• Personal Secure Drive</li> </ul>			
<b>PSD</b>	Personal Secure Drive ( * .FSF) * .FSF	PSD : PSDRecovery /L	<b>PSD</b>	PSD PSD PSD  : PSDRecovery /M: .FSF [X:]

# PSD

PSDRecovery.exe EFS cipher.exe



## **PSDRecovery /A:.CER[/ID:driveID]**

EFS Windows

Personal Secure Drive \*.CER

.CER[/ID:driveID]

.CER

: driveID Personal Secure Drive

## **PSDRecovery /D:[/ID:driveID]**

## **PSDRecovery /D:[/ID:driveID]**

EFS Windows

PSD ( PSDRecovery /V )

PSDRecovery /V

PSDRecovery /V

/ID Personal Secure Drive

## **PSDRecovery /L**

Personal Secure Drive ID

## **PSDRecovery /M:.FSF [X:]**

PSD

.FSF

PSDRecovery /L PSD

X

()

## **PSDRecovery /R:**

EFS Windows

PSD () \*.PFX () \*.CER

0

**PSDRecovery /V[/ID:driveID]**  
EFS Windows

PSD :

/ID Personal Secure Drive



©Infineon Technologies AG

**Infineon Security Platform**



# (EFS)

(EFS Encrypting File System) NTFS

EFS 1 ( PC ) EFS

EFS

:

- EFS
- Windows Home (EFS)



©Infineon

---

Technologies AG

**Infineon Security Platform**

# EFS

Microsoft (EFS Encrypting File System)  
Microsoft EFS Microsoft Windows F1

- () []
- 
- 
- []
- 
- EFS TCP/IP Internet Protocol Security (IPSec)  
PPTP 2
- : Windows Home (EFS)

---

Technologies AG



**Infineon Security Platform**

(EFS)

(EFS) EFS

- NTFS  
Windows 2000 / XP NTFS Windows 2000 /  
XP NTFS
- FAT  
EFS FAT  
1 FAT  
FAT ()
- Windows EFS (  
) OS
-

- Microsoft EFS

- 

- /

- EFS EFS

- 

EFS Microsoft EFS Microsoft Windows  
F1

EFS                     

: Windows Home (EFS)



©Infineon Technologies AG

**Infineon Security Platform**



1

[Microsoft Windows Mail/Outlook](#)

[Mozilla Thunderbird](#)



©Infineon

---

Technologies AG

**Infineon Security Platform**

# Windows Mail/Outlook Express/Outlook

Windows Mail/Outlook E:

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_



©Infineon

---

Technologies AG

**Infineon Security Platform**

Outlook Windows Mail/Outlook Express  
Outlook Windows Mail/Outlook Express 1

:

+ **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

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_



©Infineon

---

Technologies AG

**Infineon Security Platform**

Mozilla Thunderbird Mozilla Thunderbird

1

:

# Mozilla Thunderbird

1. Mozilla Thunderbird

2. > ...

3.

4. ... ()

5.

A.

B. ()

PKCS #11 [PKCS #11 Mozilla Firefox](#)



©Infineon

---

Technologies AG

**Infineon Security Platform**

# Mozilla Thunderbird

1. Mozilla Thunderbird

2. > >

3.

4.

5.

6. >



©Infineon

---

Technologies AG



**Infineon Security Platform**

# Mozilla Thunderbird

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



©Infineon Technologies AG

**Infineon Security Platform**

# Microsoft Word

Microsoft Word

Microsoft Word 2000 Microsoft Word XP

---

Technologies AG



©Infineon

**Infineon Security Platform**

# Microsoft Word

Microsoft Word

Microsoft Word  
Microsoft Word

**3**



©Infineon

---

Technologies AG

**Infineon Security Platform**

# Microsoft Word

1. > >
2. 0



1.

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

3.

4. **OK**

5.

6.

## Microsoft Word 2007 ()

- 1.
2. > >
- 3.
4. **Visual Basic**
- 5.
6. Visual Basic > ...
- 7.
- 8.
- 9.
10. **OK**
11. **OK**
- 12.
13. **Microsoft Word**

()

1.

2. > >

3.

4. **Visual Basic** Visual Basic

: **Visual Basic** > > **Visual Basic Editor**

5.

6. Visual Basic > ...

7.

8.

9.

: ... **OK**

10. **OK**

11. **OK**

12. **OK**

13. **Normal**

: **Normal ( Normal.dot)** **Document ()**

**Microsoft Word**

14. > **Microsoft Word** Microsoft Word



# **Infineon Security Platform**

Security Platform Security Platform (Microsoft Crypto-API PKCS #11 Crypto-API Cryptographic Service Provider) Trusted Platform Module

- [Web / \(\)](#)
- [\(VPN\)](#)
- [LAN LAN](#)

	<b>Security Platform</b>		
Web / ()	Infineon TPM Cryptographic Provider  Infineon TPM RSA and AES Cryptographic Provider (CSP)	SSL/TLS	
Web / ()	Infineon TPM PKCS #11 Provider	SSL/TLS	
VPN	Infineon TPM Cryptographic Provider  Infineon TPM RSA and AES Cryptographic Provider (CSP)	IPsec	
VPN	Infineon TPM Platform Cryptographic Provider (CSP)	IPsec	
LAN LAN	Infineon TPM Cryptographic Provider	LAN: IEEE 802.1X EAP-TLS	

	Infineon TPM RSA and AES Cryptographic Provider ( CSP)	LAN: IEEE 802.1X EAP-TLS	
LAN LAN	Infineon TPM Platform Cryptographic Provider ( CSP)	LAN: IEEE 802.11 EAP-TLS LAN: IEEE 802.1X EAP-TLS	



**Infineon Security Platform**





ID (CA)

Web () (CA)  
(Web) () Web

Web () (SSL)

()

()

()

Active Directory  
(IIS) Internet Explorer

- [IIS Active Directory](#)
- [Internet Explorer](#)

Mozilla Firefox PKCS #11

- [Mozilla Firefox](#)
- [Mozilla Firefox](#)



©Infineon Technologies AG

**Infineon Security Platform**

# Internet Explorer

Web Internet Explorer

Internet Explorer Microsoft TechNet

---

Technologies AG



©Infineon

**Infineon Security Platform**

# IIS Active Directory

Windows 2000 / XP Windows 2000 / XP Active Directory  
IIS ( )

IIS Active Directory  
Active Directory IIS

: IIS Web Secure Sockets Layer (SSL) CA  
SSL

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

---

Technologies AG



©Infineon

**Infineon Security Platform**

# Mozilla Firefox

Web Mozilla Firefox

1

Web () Web Web

[Mozi](#)



©Infineon

---

Technologies AG



**Infineon Security Platform**

# Mozilla Firefox

0

: ( ) 0

: Web SSL (Secure Sockets Layer) (CA) SSL

---

Technologies AG



©Infineon

**Infineon Security Platform**

(VPN)

(VPN: Virtual Private Network) ()  
VPN

VPN (VPDN: Virtual Private Dial-up Network)  
VPDN LAN  
VPDN VPN (ESP) ESP  
(NAS)

---

Technologies AG



©Infineon

**Infineon Security Platform**

(EAP)

(EAP) PPP (Point-to-Point) (VPN: Virtual Private Network)

EAP VPN EAP EAP (VPN)

EAP (CA: Certificate Authority) Security Platform VPN EAP EAP (X.509)

---

Technologies AG



©Infineon

# **Infineon Security Platform**

# EAP VPN

Infineon Security Platform  
Trusted Platform Module



Security Platform

[Cryptographic Service Provider](#)

VPN Microsoft TechNet Microsoft VPN Microsoft  
Windows F1

(VPN) VPN VPN

EAP VPN

Microsoft Windows Microsoft TechNet

EAP

- VPN
- (EAP)
- 



VPN VPN Security Platform

[Cryptographic Service Provider](#) 1

EAP



©Infineon

Technologies AG



**Infineon Security Platform**

# LAN

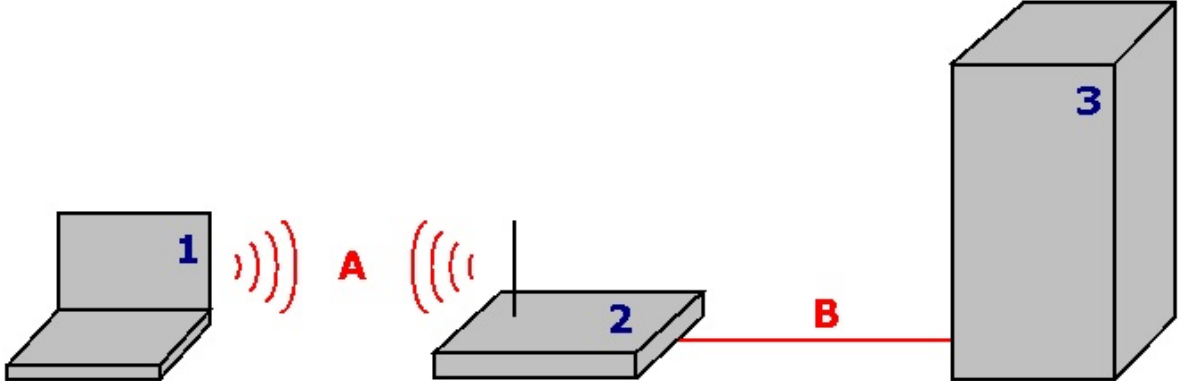
Security Platform LAN (IEEE 802.1x EAP-TLS) LAN  
(IEEE 802.1x EAP-TLS) Security Platform  
Cryptographic Service Providers (CSP) 1

LAN

# LAN

LAN LAN ()  
 LAN

**IEEE 802.11** (wireless fidelity, "Wi-Fi") LAN Wi-Fi  
 Protected Access (**WPA**) Wired Equivalent Privacy (**WEP**)



1	LAN	Security Platform PC Trusted Platform Module LAN ( A)
2		LAN ( B) LAN
3	RADIUS	Microsoft Windows 2003 Server (IAS) RADIUS

## LAN

- Microsoft Developer Network (MSDN) Microsoft Windows Help (" ")
- Wi-Fi Alliance
- Wireless LAN Association (WLANA)

# Security Platform LAN



:

- LAN LAN Trusted Platform Module Security Platform PC
- Security Platform

[LAN](#)



©Infineon Technologies AG

# **Infineon Security Platform**

# LAN

LAN LAN (IEEE 802.1X) Security Platform  
(Cryptographic Service Provider ) LAN

# LAN

<b>1.</b>	LAN Security Platform
<b>2.</b> LAN	
<b>3.</b> LAN	LAN Security Platform



LAN (CA)

.LAN RADIUS (CA)



**Cryptographic Service Provider :**

Cryptographic Service Provider

- CSP ( *Infineon TPM Cryptographic Provider*  
*Infineon TPM RSA and AES Cryptographic Provider*)
- CSP ( *Infineon TPM Platform Cryptographic*  
*Provider*)  
CSP

# LAN

LAN LAN LAN

LAN

- Microsoft Windows ( " ) LAN

- 

- **IEEE 802.1x**

- **EAP**

- 

- 



# LAN

LAN LAN

LAN

- Microsoft Windows (" ") LAN
- ""



©Infineon Technologies AG

**Infineon Security Platform**

(FAQ)

[\(FAQ\)](#)

---

---

Technologies AG



# **Infineon Security Platform**

(FAQ)

[Infineon Security Platform](#)

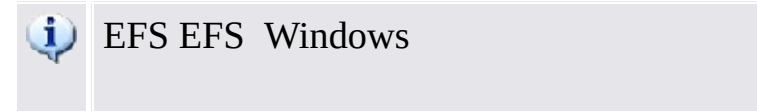
[Infineon Security Platform](#)

[Internet Explorer](#)

[EFS](#)

[EFS](#)

[Infineon Security Platform Infineon Security Platform](#)



**Infineon Security Platform**

2

- **Windows Windows**
- **Infineon Security Platform**  
"%AppData%\Infineon\TPM Software 2.0"

**Security Platform**

**Infineon Security Platform**



[Trusted Compting Management Server](#)



---

## Infineon Security Platform

Security Platform  
Infineon Security Platform  
BIOS Trusted Platform Module



Security Platform  
Infineon Security Platform

: XML  
:SPSystemBackup.xml SPSysBackup

: Security Platform Security Platform

:

**i) Windows 7 Vista:** \\%ALLUSERSPROFILE%\Infineon\TPM Software  
2.0\RestoreData\

**ii) Windows XP Professional, Windows 2000 :**

\\%ALLUSERPROFILE%\<Application Data>\Infineon\TPM Software  
2.0\RestoreData\

:

**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 :**

\\%ALLUSERPROFILE%\<Application Data>\Infineon\TPM Software  
2.0\BackupData\<Machine SID>\System\SHBackupSys.xml  
\\%ALLUSERPROFILE%\<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 Provider :** \\%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** Personal Secure Drive

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Infineon\TPM Software\PSD]  
[HKEY\_CURRENT\_USER\SOFTWARE\Infineon\TPM Software\PSD]

**Personal Secure Drive :**

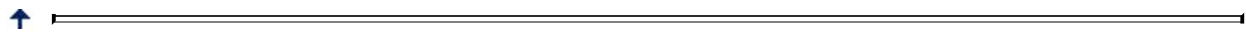
x:\Security Platform\Personal Secure Drive\System Data  
x: Personal Secure Drive Personal Secure Drive  
Personal Secure Drive

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



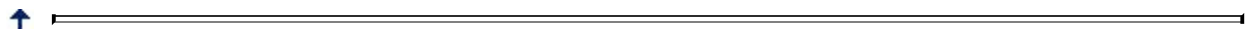
**Internet Explorer**

Internet Explorer Internet Explorer



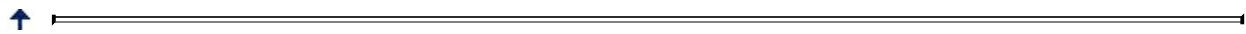
**EFS**

EFS EFS



**EFS**

EFS [Cryptographic Service Provider](#)  
EFS



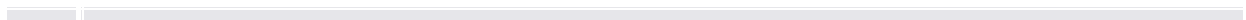
**Infineon Security Platform Infineon Security Platform**

Infineon Security Platform Infineon Security Platform

Infineon Security Platform [Infineon Security Platform](#)

Infineon Security Platform  
Infineon Security Platform

Security Platform Infineon Security Platform





- Security Platform
- [Trusted Computing Management Server](#)



## Security Platform

Infineon Security Platform

Security Platform



[Trusted Computing Management Server](#)



(

) :

- (: ) ( ) Platform

Platform

- 
- 

### **GeneratePubKeyArchive.vbs:**

```
'GeneratePubKeyArchive.vbs <.xml > <.xml >
```

```
'<.xml > :
```

```
' - SPPwdResetToken.xml
```

```
' - SPEmRecToken.xml
```

```
' - SPGenericToken.xml
```

```
'<.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 & " ""<.xml >"" ""<
.xml >""""
    WScript.Quit
End If
Set MPBase = WScript.CreateObject("IfxSpMgtPrv.MgmtProvider")
Set MPToken = MPBase.GetInterface(10)
' CreationFlags: = 0, = 1
CreationFlags = 0
ReservedFlag = 0
MPToken.CreatePublicKeyFile WScript.Arguments(0), WScript.Arguments(1),
CreationFlags, ReservedFlag
'
WScript.Echo ""

```



Trusted Computing Management Server



©Infineon Technologies AG

# **Infineon Security Platform**

Infineon Security Platform

[Trusted Platform Module](#)

[Infineon Security Platform Security Platform](#)


[Infineon Security Platform](#)

[EFS Infineon Security Platform](#)

[EFS](#)

[Infineon Security Platform EFS](#)

[EFS?](#)

	Windows Home EFS EFS Windows Home
---	-----------------------------------

**Trusted Platform Module**


Security Platform Security Platform

Infineon Security Platform ("Storage Root Key"SRK) Trusted Platform Module

[Security Platform](#)

Security Platform ()  
Infineon Security Platform

() Security Platform

 [Trust Domain Security Platform](#)  
Trust Domain ( [Trust Domain Security Platform](#) )



**Infineon Security Platform Security Platform**

Security Platform Security Platform

Security Platform



Trust Domain Trusted Platform Module  
 ( Infineon TPM Professional Package Trusted  
 Domain Server Windows Vista  
 (TPM) )



## **Infineon Security Platform**

Trusted Platform Module Security Platform

Infineon Security Platform

Infineon Security Platform [Infineon Security Platform](#)

ID



Trusted Computing Management Server



## **EFS Infineon Security Platform**

()



**EFS**

EFS

%AppData% ("Application Data")

EFS

(EFS) Microsoft Developer Network (MSDN)



## **Infineon Security Platform EFS**

**EFS ?**

**EFS**

**:** **Infineon Security Platform**

**Windows 2000 :** **Security Platform**

**:**



**©Infineon Technologies AG**



## **Infineon Security Platform -**

# Infineon Security Platform

Infineon Security Platform

# Microsoft (MMC)

[Microsoft \(MMC\)](#) Security Platform  
Security Platform

- Trusted Platform Module
- (EFS) Personal Secure Drive (PSD)

## PKCS #12 Security Platform

- : Security Platform  
Trusted Platform Module
- : EFS PSD (CA)




**EFS :**

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

... [EFS](#)  
EFS EFS PSD

[URL](#)

	EFS PSD
	PC ( : )     EFS PSD
...	
...	PKCS #12 Security Platform PKCS #12 Trusted Platform Module _____
<input checked="" type="checkbox"/>	<i>Infineon TPM Cryptographic Provider</i>
<input checked="" type="checkbox"/> PKCS #11	PKCS #11 Security Platform
	Trusted Platform Module Microsoft
	PC

	<p>EFS PSD Trusted Platform Module</p> 
<input type="checkbox"/>	
<input type="checkbox"/> ...	<p>(CA)</p>  Web <a href="#">EFS</a>
<input type="checkbox"/>	<p>Security Platform Microsoft (CA) CA</p>  : <ul style="list-style-type: none"> <li>• CA : CA</li> <li>• <a href="#">EFS</a> CA</li> <li>• EFS <a href="#">EFS</a></li> </ul>
<input type="checkbox"/>	EFS PSD
<input type="checkbox"/>	EFS PSD





## **Infineon Security Platform -**



--

<input checked="" type="checkbox"/>	<p>...</p> <p>- -</p>



©Infineon Technologies AG