

Infineon Security Platform



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 ExpressMicrosoft Outlook
Mozilla Thunderbird
- Mozilla Firefox Internet Explorer Web 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 Integration Services
- Personal Secure Drive

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

- .
- .
- .

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

Security Platform

Technologies AG



Infineon Security Platform

Trusted Platform Module

TCG TCG

Trusted

Platform ModuleTPM

PKI

TCG Infineon Infineon Security Platform Infineon
Security Platform RSA SHA-1 MD-5TRNG
SPA DPA

Trusted Platform Module



Technologies AG

Infineon Security Platform

Microsoft Windows

Microsoft Windows

Windows Vista IT “”Windows

Windows  [Infineon Security Platform](#) Security Platform



- Windows 7
- Windows

Microsoft BitLocker

Microsoft [BitLocker](#) Windows Vista BitLocker Trusted
Platform Module Trusted Platform Module

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

(TPM)

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

Windows Vista TPM TSS TPM Windows



©Infineon

Technologies AG

Infineon Security Platform -

Server Integration Services Security Platform Trust Domain



Trusted Computing Management Server

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

Security Platform Trust Domain

	AppletSecurity Platform Security Platform	Security Platform Trusted Computing Management Server
Quick Initialization Wizard		Trust Computing Management Server takes
	Security Platform	Trust Domain Security Platform
	Security Platform Security Platform	Trusted Computing Management Server
		Trusted Computing Management Server
	Personal Secure Drive (PSD)	Server Integration Services Personal Secure Drive (PSD)
		Trusted Computing Management Server
PKCS #12	Personal Information Exchange Security Platform	
	Security Platform	



©Infineon Technologies AG

Infineon Security Platform

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

12. Infineon Security Platform

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

14. , **readme**

15.



©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 Infineon Security Platform

- Infineon Security Platform



Trust Domain Security Platform

[Infineon Security Platform](#)

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

[Trusted](#)

Infineon Security Platform

Security Platform



©Infineon Technologies AG

Infineon Security Platform

Security Platform

- Security Platform Windows Windows
-
- Security Platform
-
-

	...			
Security Platform	Windows	Security Platform	Security Platform Windows Security Platform	
Security Platform “”	Windows	Windows		Windows
Security Platform “”	Windows	Security Platform Security Platform	Security Platform Windows Security Platform	
EFS/PSD “”		EFS/PSD EFS PSD	EFS/PSD	



Infineon Security Platform

Infineon Security Platform Security Platform

Infineon Security Platform

USB PIN

“”

PIN PIN PIN

Security Platform

-
-

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>Microsoft "Trusted Platform Module (TPM) Management"</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 Security Platform</p> <p>Security Platform</p> <p> Security Platform Trusted Computing Management Server</p>
		<p>Security Platform Security Platform</p> <p> Trusted Platform Computing Management Server</p>
/		<p>Security Platform Security Platform Quick</p>
		Security Platform

		 Trusted Computing Management Server
		Security Platform
	/	 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



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

Security Platform

Security Platform	
	Security Platform
	Security Platform
	<ul style="list-style-type: none"> • "" SPSysSystemBackup.xml SPSysSystemBackup Security Platform Security Platform Security Platform • SPBackupArchive.xml Security Platform Security Platform Security Platform
	Security Platform
	Trusted Platform Module Security Platform Security Platform
	<ul style="list-style-type: none"> • • SPEmRecToken.xml/ SpToken_<PCName>.xml Security Platform
Personal Secure Drive	
	PSD
	PSD PSD <ul style="list-style-type: none"> • PSD • PSD PSD Personal Secure Drive
	<ul style="list-style-type: none"> • PSD • PSD SpPSDBackup.fsbSecurity Platform PSD

'''	
	Personal Secure Drive (PSD)

	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 Settings Tool
- **Security Platform**
-
-
- XML
SPSystemBackup.xml e.g.
SPSystemBackup
\\%ALLUSERSPROFILE%\My Documents\Security Platform
- 12:00 ...
-
- SPEmRecToken.xml
-
-
- Security Platform

Security Platform - - ...

- Infineon Security Platform Settings Tool
- ...
- XML
SPSystemBackup.xml e.g.
SPSystemBackup

	<p>\\%ALLUSERSPROFILE%\My Documents\Security Platform</p> <ul style="list-style-type: none"> • 12:00 ... • • • Security Platform <p> Trusted Computing Management Server</p>
<p>“”</p>	
	<ul style="list-style-type: none"> • Infineon Security Platform Settings Tool - - ... • ... • ... • SpBackupArchive.xml • Personal Secure Drive Personal Secure Drive • • <p> Personal Secure Drive (PSD)Trusted Computing Management Server Personal Secure Drive (PSD)</p>
<p></p>	<p>- - ...</p>
<p>“”</p>	

- Infineon Security Platform
Settings Tool [-- -- ...](#)

- ...

- ...
SPBackupArchive.xml

-

-

-

- Personal Secure Drive
Personal Secure Drive
[Personal Secure Drive](#)

-

-

- Security Platform
Security Platform

-

- – **Security Platform**

- 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 Trusted Platform Module Infineon
Security Platform Trusted Platform Module

Infineon Security Platform Infineon Security Platform
Infineon Security Platform Security Platform

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

[Security Platform](#)



.Trusted Computing Management Server Personal Secure
Drive (PSD)

Trusted Platform Module Security Platform
Security Platform Security Platform



Trusted Platform Module Security Platform

Platform

-
- `SpUserWz.exe /forceinit`



Infineon Security Platform

Trusted Platform Module Infineon Security Platform

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)

1 - Trusted Platform Module	
Trusted Platform Module BIOS Infineon Security Platform	
2 - Security Platform	
Trusted Platform Module Security Platform	Infineon Security Platform Infineon Security Platform Security Platform

Infineon Security Platform	
Infineon Security Platform Infineon Security Platform	Security Platform



©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 -

Infineon Security Platform

Infineon Security Platform

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

- USB 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*
- PSD PSD PSD [Personal
Secure Drive](#)



Infineon Security Platform



Trusted Computing Management Server 3 4

1 -	
Trusted Platform Module –	<p>Infineon Security Platform</p> <ul style="list-style-type: none"> • Infineon Security Platform Settings Tool • ... • SpPubKeyArchive.xml
2 -	
1 Infineon Security Platform	<p>Infineon Security Platform</p> <ul style="list-style-type: none"> • Infineon Security Platform Settings Tool • ... • ... • SpPubKeyArchive.xml • •
1 2 -	
1 2 Infineon Security Platform Infineon Security Platform DCOM Infineon Security Platform	<p>Infineon Security Platform</p> <ul style="list-style-type: none"> • Infineon Security

- Infineon Security Platform

- Infineon Security Platform

- *SRK*

- DCOM Microsoft
Windows XP

- DCOM

-

1 2

Platform Settings Tool

- ...

- ...

-

-



Personal Secure Drive Personal Secure Drive PSD
SpPSDBackup.fsb PSD

1 -

Infineon Security Platform

Infineon Security Platform

- Infineon Security Platform Settings Tool

- ...

-

-

- **SpMigrationArchive.xml**

-

-

-

PSD

2 -

“”

Infineon Security Platform

- Infineon Security Platform Settings Tool

- ...


-

- **SpMigrationArchive.xml**

-

-

- Security Platform

	<ul style="list-style-type: none"> • • Security Platform  Personal Secure Drive
3 -	
	<ul style="list-style-type: none"> • Infineon Security Platform Settings Tool • ... • Security Platform - ... •
4 - - Personal Secure Drive	
Personal Secure Drive	Personal Secure Drive Personal Secure Drive Personal Secure Drive Personal Secure Drive <i>Personal Secure Drive</i> Personal Secure Drive SpPSDBackup.fsb Personal Secure Drive



Infineon Security Platform

Infineon Security Platform

Security Platform Security Platform



Trusted Computing Management Server

Security Platform Security Platform

Security Platform

Security Platform

- Security Platform Security Platform

1.



Security Platform

Security Platform

- Infineon Security Platform Settings Tool

-
-
-

SPPwdResetToken.xml

-
-
-

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

- Infineon Security Platform Settings Tool

- ...
-
-

SPPwdResetToken.xml

-
-
-

2.



- Infineon Security Platform Settings Tool

-
-

SPPwdResetSecret.xml

-
- Security Platform
-

- - ...

- Infineon Security Platform Settings Tool

- ...
-

SPPwdResetSecret.xml

-
-
-
-

3.

- - ...

- Infineon Security Platform Settings Tool

- ...
-
-

SPPwdResetToken.xml

-

SPPwdResetCode.xml

-

	<ul style="list-style-type: none"> • Infineon Security Platform Settings Tool • ... • • • • SPPwdResetToken.xml • • SPPwdResetSecret.xml • • •
<p>4.</p>	<p><u>- - ...</u></p> <ul style="list-style-type: none"> • Infineon Security Platform Settings Tool • ... • SPPwdResetSecret.xml • SPPwdResetCode.xml • • •



Infineon Security Platform



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

“”

Security Platform . TCG 1.2 Security Platform

-
-
-

Security Platform

-
-
- Microsoft
-
-
-

Infineon Technologies AG

Technologies AG



©Infineon

Infineon Security Platform

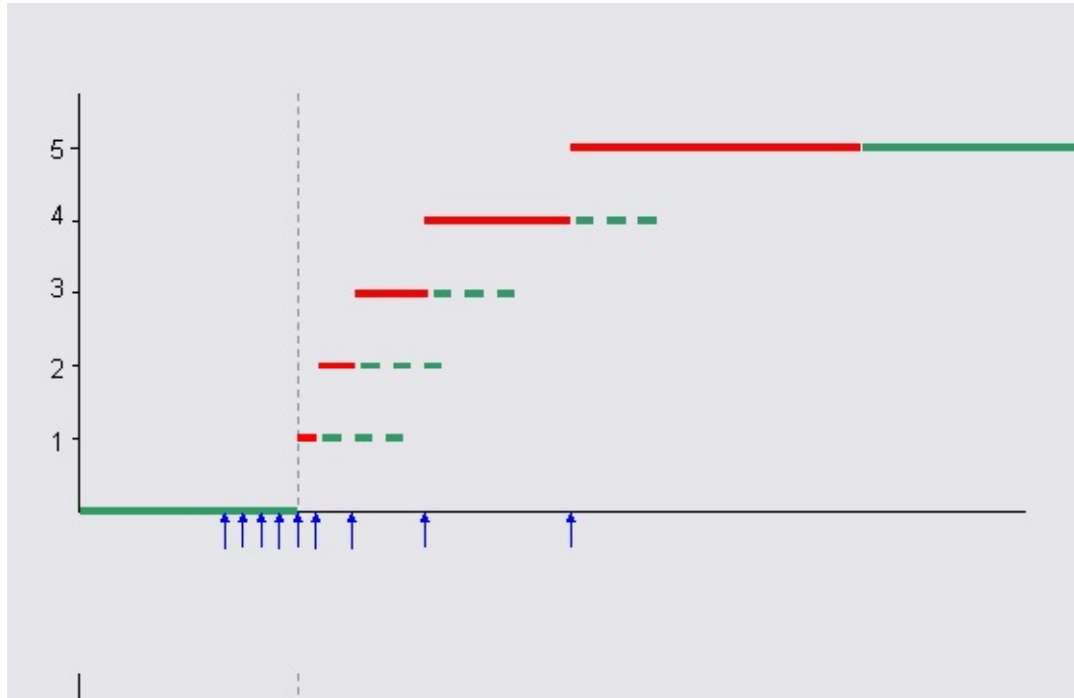


- Trusted Platform Module 1.2 Security Platforms Security Platform Infineon Trusted Platform Module 1.2 Security Platforms
- Security Platform

Security Platform

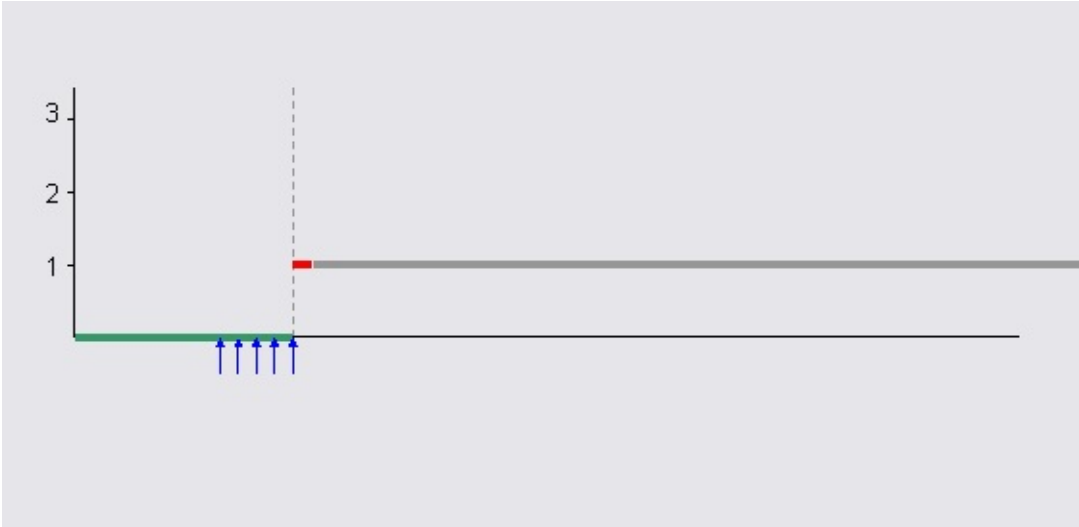
- Security Platform , Security Platform Security Platform
-
-
- Security Platform

Security Platform

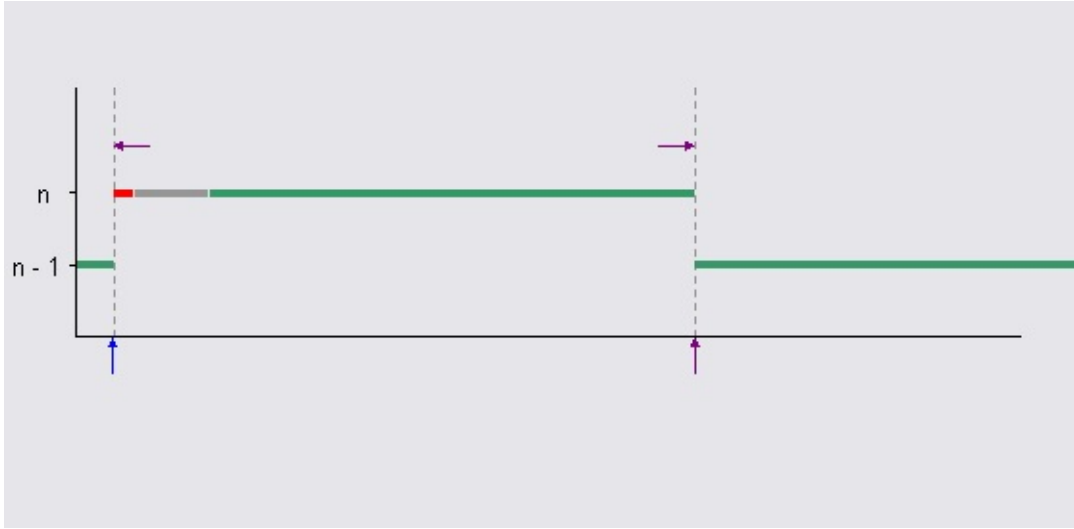


Security Platform


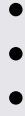
Security Platform



Security Platform Security Platform



() ()

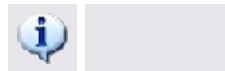
Security Platform



Security Platform

Infinion Trusted Platform Module Trusted

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

Security Platform Security Platform

:

Security Platform [Security Platform](#)

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



Security Platform

:
Trusted Computing Management Server :

-
- Trust Domain Trust Domain



-resetattack /resetattack Security Platform
SpTPMWz.exe Security Platform

- Security Platform Security Platform
-
-



Infineon Security Platform



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



- .

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





Infineon Security Platform



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

Security Platform

<p>1.</p>	<p>Security Platform Windows BitLocker PIN</p> <ul style="list-style-type: none"> • Trusted Platform Module • "" • . <p>"F5"</p> <p> Trusted Platform Module</p>
<p>2. Security Platform</p>	<p></p>



Infineon Security Platform

Infineon Security Platform



Security Platform

Infineon Security Platform

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



©Infineon

Infineon Security Platform

Security Platform

Security Platform Infineon Security Platform



Security Platform
Security Platform Platform

Security Platform

“”

-
-
-

Security Platform

Windows	Security Platform /Security Platform
Windows	Windows Trusted Platform Module
Security Platform	<u>Platform</u> . Security Platform
	PKCS #12 Security Platform
Security Platform	Security Platform /Security Platform
Trusted Platform Module	<ul style="list-style-type: none"> • Security Platform Infineon Security Platform • Trusted Platform Module Infineon Security Platform <p>Trusted Platform Module</p> <ul style="list-style-type: none"> • Trusted Platform Module • Trusted Platform Module • <p> Infineon Security Platform</p>
	Security Platform
	<ul style="list-style-type: none"> • •



Infineon Security Platform

Security Platform Security Platform


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

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



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
USB	
<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

☒☒	.
☒☒	
USB	
☒☒	.
☒☒	
☒☒ <i>PIN</i>	USB PIN
☒☒	.
☒☒	
☒☒	
	



☒☒	.
☒☒	
☒☒	
USB	
☒☒ <i>PIN</i>	USB

	PIN
☒	
☒	
☒	
☒	
☒	
☒	
☒	



/

☒	
☐ ☐	
☒	
USB	
☒ <i>PIN</i>	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 Microsoft Trusted Platform Module (TPM) Management
“”“” ”		Infineon Security Platform Security Platform “” Security Platform “ ”
PKCS #12		PKCS #12

- Windows Windows Security Platform
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">• Infineon Security Platform
	<ul style="list-style-type: none">•• Security Platform• Security Platform• Security Platform
	<ul style="list-style-type: none">••• Trusted Computing Management Server Personal Secure Drive (PSD)
	<ul style="list-style-type: none">• Security Platform• Security Platform Trusted Computing Management Server
	<ul style="list-style-type: none">•••• Trusted Computing Management Server
BitLocker	<ul style="list-style-type: none">• BitLocker Trusted Platform Module <ul style="list-style-type: none">• BitLocker Windows 7 Windows Vista Enterprise Ultimate• 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

TPM



©Infineon Technologies AG

Infineon Security Platform -

Infineon Security Platform

Infineon Security Platform
Infineon Security Platform

 <i>Security Platform</i>	Security Platform .
 <i>Security Platform</i>	Security Platform
 <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 Security Platform -

Security Platform

Infineon Security Platform

Trusted Platform Module

Trusted Platform Module

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

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

[Security Platform](#) *Security Platform*
-forceinit



-forceinit

- / / /
- / Trusted Computing Management Server
- / /- /- /-









©Infineon Technologies AG

Infineon Security Platform -

Infineon Security Platform

Infineon Security Platform

	<ul style="list-style-type: none">• Security Platform• Infineon Security Platform Trust Domain• Security Platform• Infineon Security Platform•
---	--

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






Infineon Security Platform -

Infineon Security Platform

Security Platform Security Platform Personal Secure Drive

	<ul style="list-style-type: none">• Security Platform
---	---

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

	 <ul style="list-style-type: none">• 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

Infineon Security Platform



- Security Platform
- Trusted Computing Management Server

☐ ...	
⊙	Security Platform
☐ ...	Infineon Security Platform <ul style="list-style-type: none">• Infineon Security Platform• Infineon Security Platform• Infineon Security Platform
☐ ...	Infineon Security Platform Infineon Security Platform Security Platform <ul style="list-style-type: none">• Infineon Security Platform• Infineon Security Platform•
⊙	Security Platform

☐ ...

[Infineon Security Platform](#)



- Infineon Security Platform
- Infineon Security Platform

☐ ...

Infineon Security Platform Infineon Security Platform XML



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



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 Applet



- BitLocker Windows 7 Windows Vista Enterprise Ultimate
- .

BitLocker

abc...	BitLocker
l...	Microsoft BitLocker Applet
	 Trusted Platform Module



©Infineon

Technologies AG




Infineon Security Platform -

Infineon Security Platform

Security Platform

Infineon Security Platform . Infineon Security Platform

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

 ...	Security Platform ()  <ul style="list-style-type: none">• Infineon Security Platform• Trust Domain Security Platform
 ...	<ul style="list-style-type: none">•••• <p>Infineon Security Platform</p>  <ul style="list-style-type: none">• Infineon Security Platform• Trusted Computing Management Server• Infineon Trusted Platform Module 1.2 Security Platform
 /...	Security Platform

	<p>Infineon Security Platform</p> <p>Security Platform Security Platform Trusted Platform Module EFSPersonal Secure Drive Security Platform</p> <p> BitLocker Windows Vista Enterprise Ultimate Security Platform BitLocker BitLocker</p> <p>BIOS Security Platform BIOS Security Platform Security Platform BIOS Platform Trusted Platform Module</p> <p> <ul style="list-style-type: none"> • BIOS Infineon Security Platform • Infineon Security Platform • Trusted Platform Module / </p>
<p>□ ...</p>	<p>Security Platform <i>SpTPMWz.exe -resetattack</i></p> <p> <ul style="list-style-type: none"> • Trusted Platform Module 1.2 Security Platform • Security Platform </p>
<p>□ ...</p>	<p>Infineon Security Platform</p> <p> <ul style="list-style-type: none"> • Windows Windows Home • Trusted Computing Management Server </p>
<p>□ ...</p>	<p>Infineon Security Platform</p> <p> <ul style="list-style-type: none"> • Windows Home • Trusted Computing Management Server </p>



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 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 Platform
- .
- . Security Platform
- .
- Trust Domain Security Platform

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

Trusted Platform

[1](#)

Trusted Platform

. [Security Platform](#)

Security Platform EFS PSD

. [Security Platform](#)



©Infineon Technologies AG

Infineon Security Platform -

USB

[Security Platform](#)
[BitLocker](#) USB


[Security Platform](#)
[Personal Secure Drive \(PSD\)](#)



©Infineon Technologies AG

Infineon Security Platform -

Security Platform



-
- Windows Home EFS
- [EFS](#) EFS
- [PSD](#) PSD
- [- - ...](#)

Security Platform

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

EFS PSD

EFS PSD

	EFS	PSD

	Security Platform Windows Home	Security Platform
	EFS NTFS	PSD NTFS
	EFS	<ul style="list-style-type: none"> • EFS EFS • EFS PSD
	web NTFS	
		Security Platform
<i>EFS</i> <i>PSD</i>	<i>My Documents</i>	<ul style="list-style-type: none"> • Windows Home EFS • Personal Secure Drive • FAT32



Infineon Security Platform -

Security Platform



Security Platform PSD



©Infineon Technologies AG

Infineon Security Platform -

...






USB

Technologies AG



©Infineon

Infineon Security Platform -

☐ ...	
☐ ...	 <p> <i>SpProtocol_<PCName>_<UserName>.txt</i> <i>SpProtocol_<PCName>_<UserName>.</i> <i><DomainName>.txt</i> </p>
☐	 USB
	USB

Infineon Security Platform -



USB

USB (HD)

USB HD

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



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



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

1. Trusted Platform Module	Trusted Platform Module
2. ?	Security Platform
3. .	Security Platform Security Platform
4. .	
5. .	
6. .	
7. .	
8. BitLocker	<p><i>BitLocker</i> <i>BitLocker</i> , ,</p> <p> <ul style="list-style-type: none"> • BitLocker Windows 7 Windows Vista Enterprise Ultimate • Microsoft BitLocker BitLocker </p>
9. .	Security Platform
10. _____	Infineon Trusted Platform Module 1.2 Security Platform

Security Platform
Platform

Security Platform _ Seci

Security Platform

Security Platform

- Security Platform _____ - - ...
- _____ - - ...
- _____ - - ...



TPM
©Infineon Technologies AG

Infineon Security Platform -

Trusted Platform Module


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

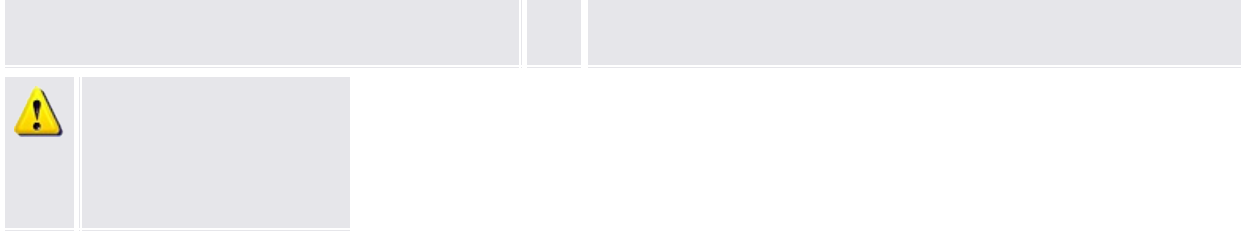
Physical Presence Interface (PPI) Trusted Platform Module 1.2
Trusted Platform Module BIOS

BIOS

Trusted Platform Module

Security Platform Trusted Platform Module

Security Platform		
Trusted Platform Module 1.2 PPI	<input type="checkbox"/>	Trusted Platform Module
Trusted Platform Module 1.2 PPI	<input type="checkbox"/>	Trusted Platform Module
Trusted Platform Module 1.2 PPI	<input type="checkbox"/>	<i>Physical Presence Interface</i> Trusted Platform Module  Trusted Platform Module
Trusted Platform Module 1.1 / PPI	<input type="checkbox"/>	BIOS Trusted Platform 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 Technologies AG




Infineon Security Platform -

Security Platform

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

 Trust Domain Security Platform

 Security Platform Storage Root Key (SRK) Trusted Platform Module 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 Pl](#)

:

- Microsoft [Trusted Platform Module \(TPM\) Management](#)
- Security Platform
- Security Platform
- Security Platform BIOS Security Platform



Trust Domain Security Platform




©Infineon

Technologies AG






Infineon Security Platform -

Security Platform

Security Platform


	Trusted Computing Management Server Security Platform <i>BitLocker</i> Microsoft
---	---






Security Platform

<input checked="" type="checkbox"/>	Security Platform 
<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> <i>BitLocker</i>	BitLocker Trusted Platform Module  BitLocker Windows 7 Windows Vista Enterprise Ultimate
<input checked="" type="checkbox"/>	 Security Platform
<input checked="" type="checkbox"/>	 Infineon Trusted Platform Module 1.2 Security Platform Security Platform



Infineon Security Platform -

 Trusted Computing Management Server

  ...	Security Platform XML , SPSystemBackup  *.xml
 ...	 PC “”“”

Infineon Security Platform -

Security Platform



- Security Platform
- Trusted Computing Management Server



	<ul style="list-style-type: none">••
<input type="text" value="abc"/> <input type="text" value="..."/>	XML CD
<input type="text" value="xxx"/>	
<input type="text" value="xxx"/>	



Infineon Security Platform -



-
- Trusted Computing Management Server



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



Infineon Security Platform -

BitLocker

BitLocker Trusted Platform Module



- BitLocker Windows 7 Windows Vista Enterprise Ultimate
- BitLocker
- BitLocker BitLocker “ ”BitLo
- Applet
- .



Microsoft BitLocker Applet



©Infineon

Technologies AG

Infineon Security Platform -



-
- Trusted Computing Management Server



Security Platform



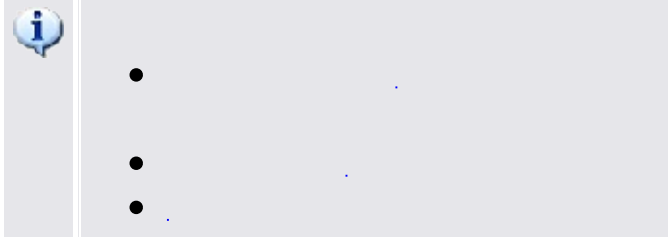
- Security Platform
-



Infineon Security Platform -

Infineon Security Platform

Infineon Security Platform Security Platform EFS
PSD Infineon Security Platform Infineon Security
Platform Security Platform



Security Platform

1.	Security Platform Security Platform Securi  “” Security Platform
2.	Security Platform
3.	Security Platform
4. Security Platform —	EFS PSD
5.	EFS PSD
6.	
7.	EFS PSD
8. Personal Secure Drive	<i>Personal Secure Drive</i>



Security Platform Security Platform

- Security Platform EFS PSD

- - ...
- - - ...
- - - ...

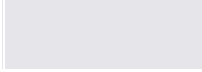
Windows Explorer Security Platform



SpUserWz.exe

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



Infineon Security Platform -





Infineon Security Platform -

Security Platform



- “”
- Security Platform

⊙ Security Platform -	Security Platform 
⊙ Security Platform	Security Platform  Security Platform Security Platform

Infineon Security Platform -



<input checked="" type="checkbox"/>	
abc <input type="text"/> ...	



Infineon Security Platform -

1

,

Technologies AG



Infineon Security Platform -

Security Platform

Security Platform



Security Platform

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

- - EFS / PSD
 - EFS PSD PSD PSD
 - EFS PSD EFS PSD PSD (EFS)
 - PSD PSD
 -
-



©Infineon Technologies AG

Infineon Security Platform -

Infineon Security Platform Infineon Security Platform



[URL](#)

...

Infineon Security Platform Infineon Security Platform



©Infineon Technologies AG

Infineon Security Platform -

/

- Microsoft Windows Mail/Outlook Express
- Microsoft Outlook 2003
- Microsoft Outlook XP
- Microsoft Outlook 2000
- Mozilla Thunderbird



Security Platform Internet

Technologies AG



©Infineon

Infineon Security Platform -




abc	
abc	/ ... /
□ ...	/ .  Microsoft Windows 7 Windows Vista "cipher.exe" Microsoft TechNet"" "cipher.exe")
	1024 2048



Infineon Security Platform

(EFS)

EFS Security Platform Microsoft EFS

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



©Infineon

Infineon Security Platform

Personal Secure Drive

Personal Secure Drive Personal Secure Drive Personal
Secure Drive Personal Secure DrivePersonal Secure Drive
Personal Secure Drive(PSD)

Personal Secure Drive



	/
PSD	1. Personal Secure Drive 2. Personal Secure Drive
PSD	1. Personal Secure Drive 2. Personal Secure Drive
PSD	1. Personal Secure Drive PSD 2. Personal Secure Drive 3. Personal Secure Drive



Infineon Security Platform

Personal Secure Drive

Personal Secure Drive PSD





 <i>Personal Secure Drive</i>	Personal Secure Drive Personal Secure Drive
 <i>Personal Secure Drive</i>	32 "My Secure Drive"
<input checked="" type="checkbox"/> <i>Personal Secure Drive</i>	PSD
<input checked="" type="checkbox"/>	PSD



Infineon Security Platform

Personal Secure Drive

Personal Secure Drive Personal Secure Drive

	(MB) USB Personal Secure Drive Personal Secure Drive  , PSD .
 PSD PSD	PSD PSD  <i>Personal Secure Drive</i> .

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

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

Infineon Security Platform

Personal Secure Drive

Personal Secure Drive PSD

 <i>Personal Secure Drive</i>	Personal Secure Drive Personal Secure Drive
 <i>Personal Secure Drive</i>	32 "My Secure Drive"
<input checked="" type="checkbox"/> <i>Personal Secure Drive</i>	PSD
<input checked="" type="checkbox"/>	PSD 

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*



©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 Infineon Security Platform
Infineon Security Platform Infineon Security Platform
Infineon Security Platform

Infineon Security Platform



- Security Platform
- Trusted Computing Management Server Infineon Security Platform

1. <u> </u>	Security Platform Security Platform
2. .	
3. .	
4. .	

- - ... - - ...



TPM
©Infineon Technologies AG

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



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



Windows 7 Windows Vista

	<u>PSD</u>	Personal Secure Drive
		Personal Secure Drive
		Personal Secure Drive
		Personal Secure Drive
		Personal Secure Drive
		Personal Secure Drive
		Personal Secure Drive
		<u>PSD</u>

Security Platform

- - ...

- - ...







Security Platform *Security Platform* Security
Platform

Security Platform . Security Platform



©Infineon Technologies AG

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"> • • Trusted Computing Management Server </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>  ...	Personal Secure Drive Personal Secure Drive
 <i>Personal Secure Drive</i>	Personal Secure Drive Personal Secure Drive Personal Secure Drive
 ...	/  *.fsb



Infineon Security Platform -



Trusted Computing Management Server






<ul style="list-style-type: none">•• <i>Trusted Platform Module</i>• <i>Security Platform</i>	<p>Security Platform</p> <ul style="list-style-type: none">• Security Platform Security Platform• <i>Trusted Platform Module</i> Security Platform Security Platform Security Platform BIOS Trusted Platform Module• <i>Security Platform</i> Security Platform Security Platform Security Platform PC <p></p>
<p>abc</p> <p>...</p>	<p> XML</p>



Infineon Security Platform

Personal Secure Drive

Personal Secure Drive PSD PSD PSD

 <i>Personal Secure Drive</i>  ...	Personal Secure Drive PSD PSD Personal Secure Drive
 <i>Personal Secure Drive</i>	Personal Secure Drive <ul style="list-style-type: none">• Personal Secure Drive PSD PSD PSD• Personal Secure Drive PSD PSD• Personal Secure Drive Personal Secure Drive Personal Secure Drive
 ...	Personal Secure Drive Personal Secure Drive PSD
 ...	Personal Secure Drive <ul style="list-style-type: none">• PSD• PSD• PSD PSD







©Infineon Technologies AG

Infineon Security Platform -

/ Personal Secure Drive

Personal Secure Drive Personal Secure Drive

 ...		PSD	
	PSD		
	Personal Secure Drive Drive		P
	32 "My Secure Drive"		
<input checked="" type="checkbox"/>	PSD		
<input checked="" type="checkbox"/>	PSD		




©Infineon Technologies AG

Infineon Security Platform -



-
- Trusted Computing Management Server

abc / ID	ID  ID
abc / ID	ID




©Infineon

Technologies AG

Infineon Security Platform -



-
- Trusted Computing Management Server

abc / ID	ID  ID
□ / ID	ID



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



Windows 7 Windows Vista

Security Platform

1.	
2.	
3.	
4.	
5.	 “”




Infineon Security Platform

-




TPM
©Infineon Technologies AG

Infineon Security Platform -

	 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	
...	
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

Microsoft PKCS #12

Security Platform PC
#12 Trusted Platform Module

Security Platform PKCS #12 PKCS

1. PKCS #12	
2.	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
xx	PKCS #12



©Infineon Technologies AG

Infineon Security Platform - PKCS #12

PKCS #12

abc	PKCS #12
...	 CA
<input checked="" type="checkbox"/> PKCS #12	PKCS #12 CA PKCS 12  CA PKCS #12 CA CA → → CA → CA
<input checked="" type="checkbox"/>	



Infineon Security Platform -


Security Platform


Security Platform

TNA Security Platform
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 Computing Management Server

Security P

Infineon Security Platform -






Infineon Security Platform




Infineon Security Platform

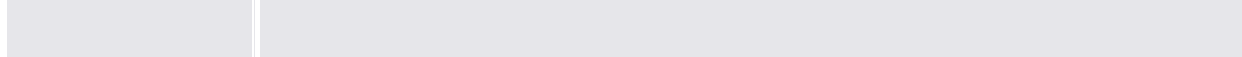
 Windows 7 Windows Vista

<i>Security Platform</i>	Infineon Security Platform 
<i>Security Platform</i>	Infineon Security Platform Infineon Security Platform Platform)  Trust Domain Security Platform
<i>Security Platform</i>	Infineon Security Platform Infineon Security Platform Security Platform 
<i>Security Platform</i>	Security Platform Security Platform  Trusted Computing Management Server
	Security Platform
<i>Personal Secure Drive -</i>	Personal Secure Drive PSD (< >) PSD
<i>Personal Secure Drive -</i>	

< > -	
<i>Personal Secure Drive -</i>	Personal Secure Drive PSD (< >) PSD
<i>Personal Secure Drive -</i> < > -	
<i>Personal Secure Drive -</i> < > -	Windows PSD PSD (< >) PSD PSD
<i>Personal Secure Drive -</i> /	Personal Secure Drive
<i>Personal Secure Drive -</i>	Personal Secure Drive
	EFS EFS
	Security Platform Security Platform • • Security Platform , Security Platform
	Security Platform PSD EFS • EFS PSD EFS PSD PSD (EFS) • PSD
<i>Security Platform</i>	Infineon Security Platform Security Platform Trusted Platform Module EFS Personal

	Secure Drive Security Platform Infineon Security Platform Trusted Platform Module 1.2 Security Platforms
<i>Security Platform</i>	Security Platform Security Platform Security Platform Security Platform 1.2 Trusted Platform Module Security Platform  Trust Domain Security Platform
<i>Security Platform</i>	Security Platform Security Platform  Trusted Computing Management Server
<i>Security Platform</i>	Security Platform  Trusted Computing Management Server
/ -	Trusted Computing Management Server “/”  Trusted Computing Management Server <ul style="list-style-type: none">•• Trusted Computing Management Server• “/”
/ -	Trusted Computing Management Server 

	<ul style="list-style-type: none"> • • Trusted Computing Management Server • “/”
/ -	 <ul style="list-style-type: none"> • • Trusted Computing Management Server • “/”
	 <ul style="list-style-type: none"> • • Trusted Computing Management Server
	
<i>Infineon TPM Strong Cryptographic Provider</i>	<u>Infineon TPM Strong Cryptographic Provider</u>
	Infineon Security Platform



©Infineon Technologies AG

Infineon Security Platform -

Infineon Security Platform

Trusted Platform Module

•

-

Infineon Security Platform

[Infineon Security Platform](#)

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 Trusted Platform Module

Technologies AG



©Infineon

Infineon Security Platform -

Infineon Security Platform

Security Platform ... [Security Platform](#)

Security Platform . Security Platform



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
IfxSpPol.admx

Security Platform

IfxSpPol.adm

1. (gpedit.msc)
- 2.
3. /...
“/”
4.
“”
5. **IfxSpPol.adm** "Security Platform"
- 6.

1. . 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>	<p>Trusted Platform Module Physical Presence Interface (PPI) Trusted Platform Module</p> <p>Trusted Platform Module</p>	
	<p>(TCG) Security Platform</p> <p> Security Platform</p>	
<i>TPM NV</i>	<p>Trusted Platform Module 1.2 (NV) NV</p> <p>NV</p> <p>NV</p> <p> Trusted Platform Module 1.2 Security Platforms</p> <p>Security Platform</p>	/
	<p>Trusted Platform Module</p> <p>Security Platform</p> <p>Windows BitLocker PIN</p> <p> Security Platforms Infineon Trusted Platform Module 1.2 Security Platform</p> <p>Security Platform</p>	<p>3</p> <p>5</p> <p>10</p>

	<p>(S3) (S4) Security Platform Security Platform</p> <p>Security Platform</p>	
	<p>class ID (CLSID) CLSID</p> <p>class ID ClassID :{76D8D888-B5AC-49FC-9408-8A45D37F3AC6}</p>	
		
SRK	<p>Trusted Platform Module Storage Root Key's(SRK) SRK Security Platform</p> <p>SRK</p> <p>SRK</p> 	

	6 6  Security Platform Trusted Computing Management Server Trusted Computing Management Server	6
	 Security Platform Trusted Computing Management Server Trusted Computing Management Server	
	Security Platform Management Provider Management Provider Management Provider Security Platform Security Platform	
	Security Platform Security Platform Security Platform : - -	
	\\BackupServer\SecurityPlatformShare\SPSystemBackup.xml XML , SPSysSystemBackup.xml SPSystemBackup  Security Platform PC	

	<p>Security Platform</p>  <p>Security Platform</p>	
	<p>\\ServerName\FolderName\FileName.xml</p> <p>Security Platform PC PC</p>  <p>Security Platform PC</p>	
	<p>Security Platform</p> <p>Security Platform</p> <p>Security Platform : <u> - - ... </u>.</p>	
	<p>\\ServerName\FolderName\FileName.xml</p> <p>Security Platform PC PC</p>  <p>Security Platform PC</p>	

	Security Platform Security Platform	---
<i>URL</i>		



Infineon Security Platform -

Infineon Security Platform



Infineon Security Platform



Trusted Computing Management Server Trusted
Computing Management Server




Security Platform

	6	6
	6	
-	<ul style="list-style-type: none"> • :42 • :7 	
	20	20
	20	
		
		
	/	/

	/ .(EFS,PSD) .	
<i>Security Platform</i>	Infineon Security Platform Security Platform Security Platform Infineon Security Platform  Security Platforms Infineon Trusted Platform Module 1.1 Security Platform	
	Security Platform	
<i>EFS</i>	Security Platform (<i>EFS</i>)  Windows Home EFS	
<i>PSD</i>	Security Platform <i>Personal Secure Drive (PSD)</i>	
	Security Platform : - -	
	Security Platform Security Platform  Security Platform	
	Infineon Security Platform	

<p><i>URL</i></p>	<p>Infineon Security Platform web web</p> <p>Security Platform</p> <p>Infineon Security Platform</p> <ul style="list-style-type: none"> • Security Platform • • EFS <i>EFS</i> 	
<p><i>EFS</i></p>	<p>EFS web EFS</p> <p>1. EFS</p> <ul style="list-style-type: none"> • • : WWW. • PC <p>2. URL EFS CA web</p> <p>https://www.companyname.com/foldername (CA) EFS</p> <ul style="list-style-type: none"> • URL • EFS • EFS Security Platform PC EFS <p>EFS EFS web EFS</p> <ul style="list-style-type: none"> • EFS EFS PSD • EFS EFS PSD <i>URL</i> <p>EFS</p>	
<p><i>EFS</i></p>	<p>EFS Security Platform</p> <p>14</p>	<p>14</p>
<p><i>EFS</i></p>	<p>EFS</p>	<p>10</p>

	10	
<i>Personal Secure Drive</i>	PSD Personal Secure Drive C: Personal Secure Drive Personal Secure Drive	
<i>PSD</i>	PSD PSD PSD PSD 5000 MB Windows 7 Windows Vista PSD 20 MB 10 MB <ul style="list-style-type: none"> • PSD 5050 MB PSD 50 MB • 5000 MB PSD 	5000 MB
	Security Platform Security Platform Security Platform Security Platform	
<i>MS-CAPI</i>	MS-CAPI 	
	/ Infineon TPM / ,	/

	Security Platform	
	Management Provider Management Provider Security Platform Security Platform	



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 CSP AES	Trusted Platform Module	Microsoft Crypto-API	<ul style="list-style-type: none"> • EFS PSD • Outlook Windows Mail/Outlook Express (S/MIME) • Internet Explorer SSL/TLS • Microsoft Internet Explorer (CA) • Microsoft Word • Microsoft Crypto-API Checkpoint VPN • Microsoft Crypto-API Entrust • Adobe Adobe • EAP-TLS
Infineon TPM RSA and AES Cryptographic Provider CSP AES Windows 2000			
Infineon TPM PKCS		PKCS #11	<ul style="list-style-type: none"> • Mozilla

<p>#11 Provider “TPM Cryptoki”</p>		<p>Crypto-API</p>	<p>Thunderbird (S/MIME)</p> <ul style="list-style-type: none"> • Mozilla Firefox SSL/TLS • Mozilla Firefox (CA) • CA • RSA SecurID Web • PKCS #11 Entrust
<p>Infineon TPM Strong Cryptographic Provider AES</p>	<p>Trusted Platform Module</p>	<p>Microsoft Crypto-API</p>	<ul style="list-style-type: none"> • VPN
<p>Infineon TPM Platform Cryptographic Provider (CSP)</p>	<p>Trusted Platform Module</p> <p>Trusted Platform Module CSP</p>	<p>Microsoft Crypto-API</p>	<ul style="list-style-type: none"> • IEEE 802.11 EAP-TLS WLAN RADIUS TLS • IEEE 802 EAP-TLS RADIUS TLS LAN • VPN IPsec
<p>Infineon TPM Key Storage Provider (KSP)</p>	<p>Infineon TPM</p>	<p>Microsoft Cryptography</p>	<ul style="list-style-type: none"> • Microsoft .NET 3.0

	Cryptographic Service Provider TPM RSA	Next Generation (CNG) API	• Cryptographic Service Provider
--	---	---------------------------	----------------------------------



©Infineon Technologies AG

Infineon Security Platform

Security Platform

Security Platform (TCG)

TCG (TSS)

- TSSTCG Service Provider
- TSS Core Service
- TSS Device Driver Library

TCG TCG



Trusted Platform Module



©Infineon Technologies AG

Infineon Security Platform

Server Integration Services

Server Integration Services Trusted Computing Management Server
Security Platform Trusted Computing Management Server

Client Side Control Agent Server Integration Services

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

Infineon TPM Professional Package Server Integration Services

Server Integration Services
Client Side Control Agent

ReadmeServerIntegrationService



©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](#)
- .



©Infineon

Technologies AG

Infineon Security Platform

(PKI)

Security Platform CAPKI

[Security Platform /](#)



PKI

[Windows](#)

[PKCS #11](#)

Technologies AG



©Infineon

Infineon Security Platform

-
-
-
-
- CA
- CA

-
-
-

“”CA .CA CA Internet Intranet

Technologies AG



©Infineon

Infineon Security Platform

CA

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

CA

-
-
-

CA CA CPS CA CA CPS

CA

- CA
- CA CA CA
- CA
- CA
- CA

CA CA CA



Security Platform

[Cryptographic Service Providers](#)



Infineon Security Platform

Windows (PKI)

Microsoft Windows 2000 Windows (PKI) Windows

PKI (DC) Kerberos (KDC) Windows PKI
extranet internet

Microsoft TechNet Microsoft PKI

PKI

-
-
-
-

Technologies AG



©Infineon

Infineon Security Platform

Microsoft Windows 2000 Windows 2000

CA PKI

“”

Microsoft TechNet

PKI

Technologies AG



Infineon Security Platform

CAPKICA 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 DNS CA

CA Microsoft TechNet

PKI Security Platform [Cryptographic Service Providers](#)



©Infineon

Technologies AG

Infineon Security Platform

Cryptographic Service Providers (CSP) CSP Security Platform
[Cryptographic Service Providers](#)

1. **ADSI Edit**

ADSI Microsoft Management Microsoft
Management Windows 2000 Server CD Support\Tools
Setup Windows 2000 Windows 2000
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=User

pKIDefaultCSPs

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

:
: 1, Microsoft Enhanced Cryptographic Provider v1.0
2, Microsoft Base Cryptographic Provider v1.0

:
3, Infineon TPM Cryptographic Provider

Security Platform

[Cryptographic Service Providers](#)



©Infineon Technologies AG

Infineon Security Platform

Security Platform [Cryptographic Service Providers](#)

- Microsoft Management Console
- Windows 2000 server web



©Infineon

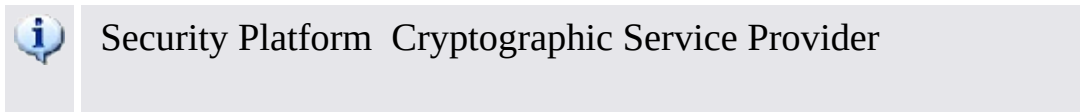
Technologies AG

Infineon Security Platform

Microsoft Management Console

CA Windows

1. Microsoft Management Console
Microsoft Management Console
2.
...
- 3.
4. Security Platform [Cryptographic Service Providers](#)
5. Security Platform Cryptographic Service Provider
CSP



- 6.
- 7.
- 8.



Infineon Security Platform

Web

Microsoft CA Microsoft Windows Microsoft Windows
Server 2003

CA web

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


 Security Platform [Cryptographic Service Providers](#)

Cryptographic Service Provider

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

MS Base Cryptographic Provider V1

Security Platform Cryptographic Service Providers
CSP Container GUID

 Security Platform Cryptographic Service Provider



Infineon Security Platform

PKCS #11 PKI

PKCS #11 PKCS #11 PKCS #11

PKCS #11

PKCS #11 PKCS #11

PKI PKCS #11 PKCS #11 LDAP

Windows 2000 / XP PKCS #11 PKCS #11 Trusted Platform Module

PKCS #11 PKCS #11

PKCS #11 public key

PKI

-
-
-
-

[Mozilla Firefox](#) Infineon Security Platform PKCS #11



Security Platform PKCS#11 Security Platform
PKCS#11 DLL (*ifxtpmck.dll*) Security Platform
system32 ifxtpmck.dll



©Infineon

Technologies AG

Infineon Security Platform

Mozilla Firefox PKCS #11

PKCS #11 PKI Infineon Security Platform PKCS #11
Infineon Security Platform Trusted Platform Module

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. **Cryptographic**

Technologies AG



©Infineon

Infineon Security Platform

Security Platform [Cryptographic Service Providers](#)

- [Sun Certificate Server](#)
- [CAPKCS #11](#)

Technologies AG



Infineon Security Platform

Sun CA

iPlanet CA Windows 2000 / XP Unix Linux

PKCS #11

Mozilla Firefox

1. Mozilla Firefox

2. Mozilla Firefox

3.

1025 SSL

https://your_server_name:1025

4.

5. CA

-

-

-

CA

CA

1. > ...

2.

3. CA

- CA web

- CA /

- CA



Infineon Security Platform

PKCS #11 CA

CA web

[Sun Certificate Server](#) CA

Service Provider

Technologies AG



©Infineon

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.

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



PSD

PSD

PSD Trusted Computing Management Server PSD



PSD

PSD USB PSD

PSD PSD



©Infineon Technologies AG

Infineon Security Platform

Personal Secure Drive

Personal Secure Drive

- AES
- RSA
- —
- —

Personal Secure Drive Personal Secure Drive

- Personal Secure Drive Windows
-
- Microsoft EFS

Trusted Platform Module

Personal Secure Drive — Trusted Platform Module TPM Trusted
Platform Module “” Trusted Platform Module

Personal Secure Drive

-
- Trusted Platform ModuleTPM
-
- Windows Personal Secure Drive
-
-

Technologies AG



Infineon Security Platform - PSD PSD

Personal Secure Drive

Personal Secure Drive

PSD PSD PSD PSD

PSD

PSD **Personal Secure Drive –**
Secure Drive - <> -

Personal Secure Drive
Personal Secure Drive

Persona

Windows Explorer PSD.

PSD

Windows PSD

Personal Secure Drive - Personal Secure Drive **Personal**
Secure Drive - <> - Personal Secure Drive

PSD

PSD **Personal Secure Drive -**
Secure Drive - <> -

Personal Secure Drive
Personal Secure Drive

Personal

PSD

PSD Security Platform

PSD

PSD Personal Secure Drive PSD

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



©Infineon Technologies AG

Infineon Security Platform

Personal Secure Drive

Personal Secure Drive

[Infineon Security Platform](#) Personal Secure Drive

Personal Secure Drive

Personal Secure Drive

“”

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

7999



©Infineon

Technologies AG

Infineon Security Platform

Personal Secure Drive

PSD Personal Secure Drive Recovery PSD Home
edition Windows XP Home Windows XP Professional
Windows Vista Basic Home Windows Vista Home Premium Home
“ PSD ” PSD



PSD :

- PSD
- PSD

PSD

[PSD](#)

PSD

PSD	EFS Windows	EFS Windows
	<ul style="list-style-type: none"> PSD PSD PSD PSD 	<ul style="list-style-type: none"> EFS Microsoft PSD PSD
PSD	<ol style="list-style-type: none"> PSD PKCS #12 PKCS #12 PSDRecovery /R:filename PSD PSDRecovery /A:filename.CER [/ID:driveID] 2 1 	<ol style="list-style-type: none"> PSD Microsoft EFS secpol.msc PSD 2 1 3 Windows 2000 EFS Windows 7 Windows Vista Windows XP Professional
	PSD PSDRecovery /V [/ID:driveID]	Microsoft EFS secpol.msc
	PSD PSDRecovery /D:[name] [number]	Microsoft EFS secpol.msc

	[/ID:driveID]	
PSD	<ul style="list-style-type: none"> • PKCS #12 • Personal Secure Drive • Personal Secure Drive 	
PSD	Personal Secure Drive * .FSF * .FSF PSD PSDRecovery /L	PSD PSD PSD PSD PSDRecovery /M:DriveImageFile.FSF [X:]

PSD

PSDRecovery.exe EFS cipher.exe



EFS Windows PSDRecovery /A:filename.CER
[/ID:driveID]

*.CER Personal Secure Drive

filename.CER	.CER
--------------	------

/ID:driveID	ID Personal Secure Drive
-------------	--------------------------

Windows Home PSDRecovery /D:name [/ID:driveID]
PSDRecovery /D:number [/ID:driveID]

PSD PSDRecovery /V

name	PSDRecovery /V
------	----------------

number	PSDRecovery /V
--------	----------------

/IDPersonal Secure Drive

PSDRecovery /L

Personal Secure Drive ID

PSDRecovery /M:DriveImageFile.FSF [X:]

PSD

DriveImageFile.FSF	PSDRecovery /L PSD
--------------------	--------------------

X	
---	--

Windows Home PSDRecovery /R:filename

PSD *.PFX *.CER

filename

Windows Home PSDRecovery /V [/ID:driveID]

PSD

/IDPersonal Secure Drive



©Infineon Technologies AG

Infineon Security Platform

EFS NTFS EFS

-
- Windows Home EFS

Technologies AG



©Infineon

Infineon Security Platform

EFS

EFS Microsoft Windows F1

-
-
-
-
-
- EFS TCP/IP — Internet Protocol Security IPsec PPTP

Windows Home EFS



©Infineon

Technologies AG

Infineon Security Platform

EFS EFS

- NTFS
Windows 2000 XP NTFS NTFS
- FAT
FAT FAT
- Windows EFS
-

- EFS

-

-

- EFS

- “”

EFS EFS Microsoft Windows F1

EFS .

Windows Home EFS



©Infineon Technologies AG

Infineon Security Platform

/

[Microsoft Windows Mail/Outlook](#)

[Mozilla Thunderbird](#)



©Infineon

Technologies AG

Infineon Security Platform

Windows Mail/Outlook Express/Outlook

Windows Mail/Outlook Express/Outlook

-
-
-



©Infineon

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 Mail

-
-
-



©Infineon

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

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. >



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 “”“”

Technologies AG



©Infineon

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.

4. **Visual Basic**

> > **Visual Basic**

Visual Basic

5.

6. Visual Basic > ...

7.

8.

9.

...

10.

11.

12.

13.

Normal.dot

Microsoft Word

14. > Microsoft Word



Infineon Security Platform

Security Platform Security Platform Microsoft Crypto-API
 PKCS #11 Crypto-API Cryptographic Service Providers Trusted
 Platform Module

- [Web / _____](#)
- [VPN _____](#)
- [WLAN _____](#)

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

LAN

Provider (Platform CSP)

EAP-TLS
LAN IEEE
802.1X EAP-TLS



©Infineon Technologies AG

Infineon Security Platform

SSL

“” IIS Active Directory 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

Microsoft TechNet Internet Explorer

Technologies AG



©Infineon

Infineon Security Platform

IIS

Windows 2000 / XP Internet (IIS) Windows 2000 / XP

IIS IIS

IIS Web (SSL) CA SSL

Microsoft TechNet “ IIS ”“Internet ”



©Infineon

Technologies AG

Infineon Security Platform

Mozilla Firefox

Mozilla Firefox

Technologies AG



©Infineon

Infineon Security Platform

Mozilla Firefox

Web SSL CA SSL

Technologies AG



Infineon Security Platform

VPN

VPN InternetVPN "" Internet

VPDN"" VPN ESPESP NAS

Technologies AG



©Infineon

Infineon Security Platform

EAP

EAP VPN EAP VPN

EAP CA Security Platform
X.509

VPN EAP EAP

Technologies AG



©Infineon

Infineon Security Platform

VPN EAP

Infineon Security Platform
Module

Trusted Platform



Security Platform

[Cryptographic Service Providers](#)

VPN Microsoft TechNet Microsoft VPN Microsoft
Windows F1

Internet Intranet VPN VPN Internet Intranet

EAP VPN Microsoft Windows Microsoft
TechNet

EAP

- VPN
- “” (EAP) SmartCard
- EAP



VPN VPN Security Platform
[Service Providers](#)

[Cryptographic](#)

EAP



©Infineon

Technologies AG

Infineon Security Platform

(WLAN)

Security Platform WLAN(IEEE 802.11 EAP-TLS) (IEEE
802.1X EAP-TLS) Security Platform Cryptographic Service
Providers (CSP)

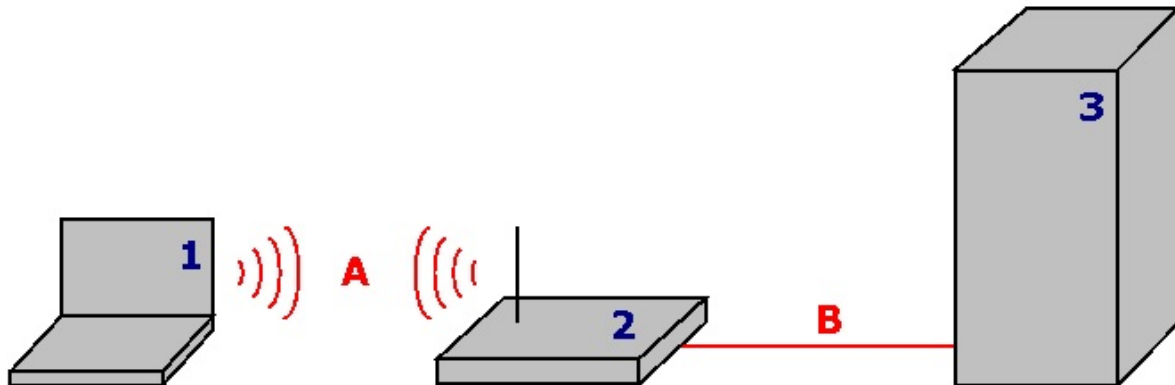
WLAN

WLAN

WLAN WLAN

IEEE 802.11 "Wi-Fi" Wi-Fi

WPAWEP



1	WLAN	Security Platform PC Trusted Platform Module WLAN	A
2		“” WLAN WLAN	B
3	RADIUS	Internet IAS Microsoft Windows 2003 Server RADIUS	

WLAN Internet

- Microsoft Developer Network (MSDN) Microsoft Windows
“”)
- Wi-Fi
- WLANA

Security Platform WLAN



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

[WLAN](#)



©Infineon Technologies AG

Infineon Security Platform

WLAN

WLAN IEEE 802.1X Security Platform Cryptographic
Service Provider WLAN

WLAN

1.	WLAN Security Platform
2. WLAN	
3. WLAN	WLAN Security Platform

WLAN . WLAN RADIUS



Cryptographic Service Provider

Cryptographic Service Provider

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

WLAN

WLAN WLAN WLAN

WLAN

- Microsoft Windows “” WLAN

-

- **IEEE 802.1x**

- **EAP**

-

-



WLAN

WLAN WLAN

WLAN

- Microsoft Windows “” WLAN
- “”



©Infineon Technologies AG

Infineon Security Platform

[\(FAQ\)](#)

Technologies AG



Infineon Security Platform

(FAQ)

[Infineon Security Platform](#)

[Infineon Security Platform](#)

[Internet Explorer](#)

[EFS](#)

[EFS](#)

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



EFS EFS Windows

Infineon Security Platform

- Windows
- Infineon Security Platform Software 2.0 `\%AppData%\Infineon\TPM`

Security Platform [___](#).



Infineon Security Platform



Trusted Computing Management Server

Infineon Security Platform

Security Platform Infineon Security Platform
BIOS Trusted Platform Module



Security Platform Infineon Security Platform

XML SPSystemBackup.xml SPSystemBackup

Security Platform Security Platform

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

ii) Windows XP ProfessionalWindows 2000
\\%ALLUSERPROFILE%\<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 ProfessionalWindows 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 Drives Personal Secure Drive Personal
Secure Drive

Trusted Platform Module

C:\WINDOWS\Tasks\Security Platform Backup 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

Infineon Security Platform Security Platform “_____” .



- Security Platform
- Trusted Computing Management Server



___ Security Platform

Infineon Security Platform

Security Platform



Trusted Computing Management Server



-

Platform

-
-

GeneratePubKeyArchive.vbs

'GeneratePubKeyArchive.vbs <Full path to Token.xml> <Full path to PubKeyArchive.xml>

'The <Full path to Token.xml> can be one of the following tokens:

' - SPPwdResetToken.xml

' - SPEmRecToken.xml

' - SPGenericToken.xml

'The <Full path to PubKeyArchive.xml> is the output, which contains the public key extracted from the input token:

' - SPPwdResetTokenPubKeyArchive.xml

' - SPEmRecTokenPubKeyArchive.xml

' - SPGenericTokenPubKeyArchive.xml

'For usage by the "Use public key of Emergency Recovery Token from archive" policy:

' - SPEmRecTokenPubKeyArchive.xml

' - SPGenericTokenPubKeyArchive.xml

'For usage by the "Use public key of Password Reset Token from archive" policy:

' - SPPwdResetTokenPubKeyArchive.xml

' - SPGenericTokenPubKeyArchive.xml

'Be sure to specify the full path e.g.:

' GeneratePubKeyArchive.vbs "c:\tmp\SPGenericToken.xml"

"c:\tmp\SPGenericTokenPubKeyArchive.xml"

If WScript.Arguments.Count <> 2 Then

 WScript.Echo "Usage:" & Wscript.ScriptName & " ""<Full path to Token.xml>"" ""<Full path to PubKeyArchive.xml>"""

 WScript.Quit

End If

Set MPBase = WScript.CreateObject("IfxSpMgtPrv.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 "Done"
```



Trusted Computing Management Server



©Infineon Technologies AG

Infineon Security Platform

Infineon Security Platform

[Trusted Platform Module](#)


[Infineon Security Platform Infineon Security Platform](#)

[Infineon Security Platform](#)

[EFS Infineon Security Platform](#)

[EFS](#)

[EFS](#)

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

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



Infineon Security Platform Infineon Security Platform

Security Platform Security Platform Security Platform

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



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%

EFS

Microsoft Developer Network (MSDN)



EFS

EFS

Infineon Security Platform

Windows 2000 Security Platform



©Infineon Technologies AG

Infineon Security Platform -

Infineon Security Platform

Infineon Security Platform

Microsoft

[Microsoft](#) 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
<input type="checkbox"/>	Trusted Platform Module Microsoft
<input type="checkbox"/>	PC EFS PSD Trusted Platform Module

	
<input type="checkbox"/>	
<input type="checkbox"/> ...	CA  EFS web
<input type="checkbox"/>	Security Platform Microsoft CA CA  <ul style="list-style-type: none"> • CA CA • EFS CA • EFS EFS
<input type="checkbox"/>	EFS PSD
<input type="checkbox"/>	EFS PSD

- - ... Security Platform

Security Platform EFS PSD

- ...



©Infineon Technologies AG

Infineon Security Platform -



“”



“”“”

- - ...



©Infineon Technologies AG