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 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 Integration Services
- Personal Secure Drive

Infineon Security Platform

Infineon Trusted Platform Module Infineon Security Platform

.

-
-
-

, .

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

Security Platform

.

.

Infineon Technologies AG

Infineon Security Platform Solution

Trusted Platform Module

.

. .

,

.

.

, , , .

(Trusted Computing Group) . TCG

. TCG **Trusted Platform Module (TPM)** ,

.

Trusted Platform Module ( ) .

3

. . Truste

(PKI) .

.

TCG . Trusted

Platform Module

. Infineon Trusted Platform Module RSA

(SHA-1 MD-5) TRNG (True Random Nu

generator) . SPA (Simple Power Analysis) DPA (Differential

Power Analysis) .

. Trusted Platform Module

.

Infineon Security Platform

Microsoft Windows

Microsoft Windows .

Windows Vista .
, "
" . Windows
, . ,

.

Windows (:
Infineon Security Platform Security Platform).

- Windows 7
  .
- Windows
  .

Microsoft BitLocker

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

TPM ( )

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

Windows Vista TPM TSS TPM
Windows .

Infineon

Technologies AG

Infineon Security Platform -

Server Integration Services Security Platform Trust Domain .

Trusted Computing Management Server

.

	. : • Trust Domain (*Trusted Computing Management Server*). • Trusted Platform Module . • Trusted Platform Module (Infineon TPM Trusted Domain , Windows *Trusted Platform Module(TPM)*). • Trust Domain . , Trust Domain .
	. : • Trust Domain (*Trusted Computing Management Server*). • Trusted Platform Module . • Trust Domain . , Trust Domain . • .

Security Platform Trust Domain .

:

.

__	. Security Platform Security Platform .	Security Platform Trusted Computing Management Server . .
____	( ).	Trust Computing Management Server .
__	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 Security Platform

Infineon Security Platform

Infineon Security Platform

. .

:
ReadmeUpgrade.txt .

1. .

: Infineon Security Platform ,
.

2. InstallShield Infineon Security Platform
.

3. .

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 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 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 Trusted Platform Module .

Infineon Security Platform . .

Security Platform (FAQ) .

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

. (Brute-Force)

PIN .

. .

Security Platform .

- .
- . .

.

. Security Platform

.

. , Security Platform

. .

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

Infineon Technologies AG

Infineon Security Platform

, Security Platform

Infineon Security Platform ,
(:). Security Platform
Security Platform . .

Security Platform .

	...	/
		( ). Microsoft "Trusted Platform Module(TPM) Management" .  __ Trusted Computing Management Server .
,	/	Security Platform , Security Platform Personal Secure Drive . . Trusted Platform Module . .  __ Security Platform , Trusted Computing Management Server .
		Security Platform (Security Platform). (Trusted Platform Module) .  __ Security Platform Trusted Computing Management Server .
		Security Platform (Security

		Platform). .  Trusted Platform Computing Server .
/		Security Platform (Security Platform . .
		Security Platform . . .  Trusted Computing Management Server .
		Security Platform . .
	/	. . .  Trusted Computing Management Server .
PKCS #12 ( )		. .

Infineon Security Platform

Security Platform

Security Platform

EFS PSD

Infineon Technologies AG

Infineon Security Platform

Security Platform

Security Platform . Security Platform
Trusted Platform Module
Security Platform .

Personal Secure Drive . Security Platform
(:) Security Platform .

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

Security Platform .

Security Platform	
	Security Platform .
	. Security Platform .
	• (" ", : SPSystemBackup.xml SPSystemBackup): Security Platform . Security Platform (Security Platform). ID ID . • (: SPBackupArchive.xml): Security Platform . Security Platform (Security Platform). ID ID .
	Security Platform .
	Trusted Platform Module . Security Platform . . Security Platform .
	• . . • (: SPEmRecToken.xml) / (: SpToken_<PCName>.xml): Security Platform . .
Personal Secure Drive	
	PSD , .

	PSD . PSD . : • PSD , . • PSD PSD Personal Secure Drive .
	• PSD . • **PSD** (: SpPSDBackup.fsb): Security 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) (: SPSystemBackup) : *\%ALLUSERSPROFILE%\My Documents\Security Platform*. • 12:00 . **...** . • . • (: SPEmRecToken.xml) . • . • . • . .

	• Security Platform . . Security Platform : ___ - - ... : • Infineon Security Platform Settings Tool . • ... . • . XML (: SPSystemBackup.xml) (: SPSystemBackup) : *\%ALLUSERSPROFILE%\My Documents\Security Platform*. • 12:00 . ... . • . • " " . • Security Platform . . __ Trusted Computing Management Server . , .
(" ")	
: .	: • Infineon Security Platform Settings Tool . ____ - - ...

	• ... . • ... (: SpBackupArchive.xml). • Personal Secure Drive (Personal Secure Drive ___) . • . • .  __ Personal Secure Drives(PSD) . Trusted Computing Management Server . PSD(Personal Secure Drive) .

: .
: .
  .
 
 	
  .
	_ - ... _____

(" ")	
: . . .	: • Infineon Security Platform Settings Tool . *Security Module - - ...* • ... . • . ... (: SPBackupArchive.xml) .

-
- .
- .
- Personal Secure Drive
  Personal Secure Drive
  (Personal Secure Dri
  _____).
-
- .
- 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 Trusted Platform Module
Trusted Platform Module Infineon Security
Platform .

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

Security Platform .

PSD(Personal Secure Drive)
Trusted Computing Management Server .

,

, __ .

.

.

Trusted Platform Module
. Security Platform
. Security Platform
. Security Platform .

(FAQ) .

:

(: Trusted Platform Module
) Security Platform .

.

(:)

. __ Security Platf
: *SpUserWz.exe /forceinit.*

:

- .
- : __ *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 . . . . FAQ .
- **:** , . Infineon Security Platform . . .
- __ PSD(Personal Secure Drive) Trusted Computing Management Server .

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 . . . , . .

Infineon Security Platform

( )

. Windows

. .

_____ .

:

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

.

.

- Personal Secure Drive .
- __ .

Infineon Security Platform

EFS PSD

EFS PSD :

- .
- .
- (EFS , PSD).
- .

Microsoft TechNet .

PSD Personal Secure Drive .

Infineon 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: • Personal Secure Drive (: USB) . • Personal Secure Drive Personal Secure Drive

. Personal Secure Drive
.
Personal Secure Drive .
Personal Secure Drive (Pers
Drive). Personal Secure Drive *Personal Secure*
Drive .

- PSD
. PSD .
PSD (Personal Secure

Infineon Security Platform

. ,
. .

	Trusted Computing Management Server . , (3 4).

1 - ID	:
. Infineon . (: Trusted Platform Module .) - .	Infineon Security Platform ( ) . : • Infineon Security Platform Settings Tool . • ... . • . **SpPubKeyArchive.xml** . : . .
2 -	**:**
. . (1). Infineon Security Platform .	() Infineon Security Platform . : • Infineon Security Platform Settings Tool . • ... . • ... . • **SpPubKeyArchive.xml**

	. • . • ID
1 2 -	**:**
. 1 2 . Infineon Security Platform . . Infineon Security Platform DCOM . Infineon ( ) . ( ). **:** • : (Infineon Security Platform) . • : Infineon Security Platform . • : *SRK* . • : DCOM (: Microsoft Windows XP). • DCOM . • . (1 2) .	() Infineon Security Platform . : • Infineon Security Platform Settings Tool . • ... . • ... . . • . • . .

	Personal Secure Drive Personal Secure Drive (: . 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 . . • . • **Security Platform** .  Personal Secure Drive . .
3 -	**:**
.	. , . : • 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 *Personal Secure Drive* . 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**) (:) . . • . : • Infineon Security Platform Settings Tool . • **...** . • . • (: **SPPwdResetToken.xml**) . . • (: **SPPwdResetSecret.xml**) . • . • . • .

4. : ( ).	- - ... ( ) : • Infineon Security Platform Settings Tool . • **...** . • (: **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 .

Infineon Security Platform

:

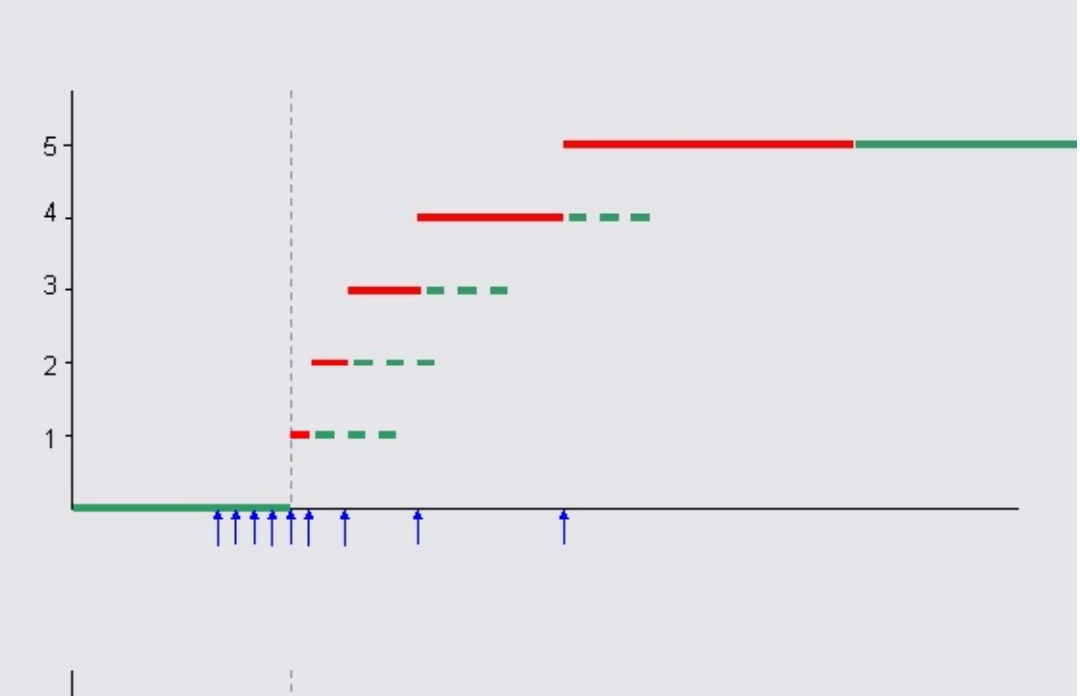
- Trusted Platform Module 1.2 Security Platform .
  Security Platform Infineon Trusted
  Platform Module 1.2 Security Platform .
- Security Platform .

Security Platform :

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

Security Platform

.

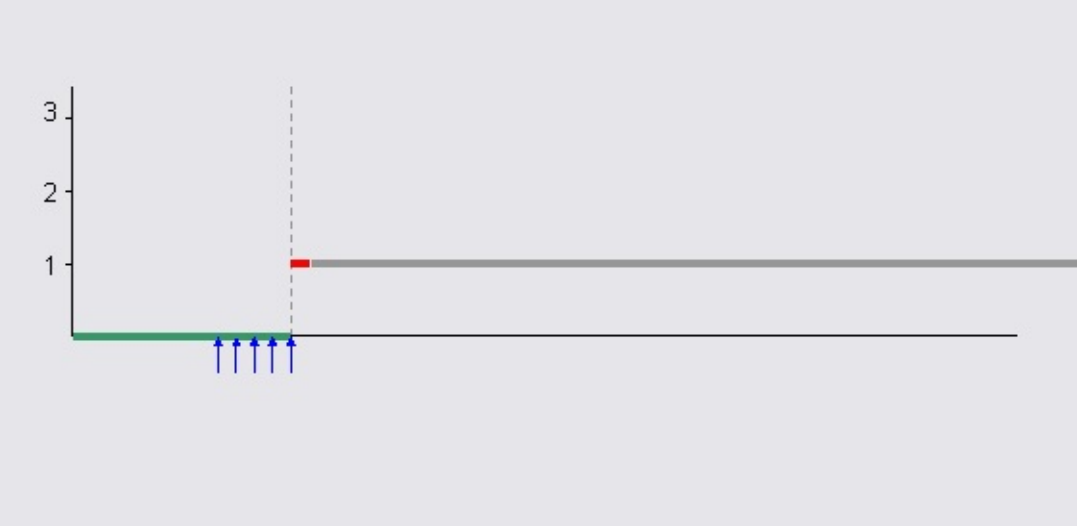


. ,

.

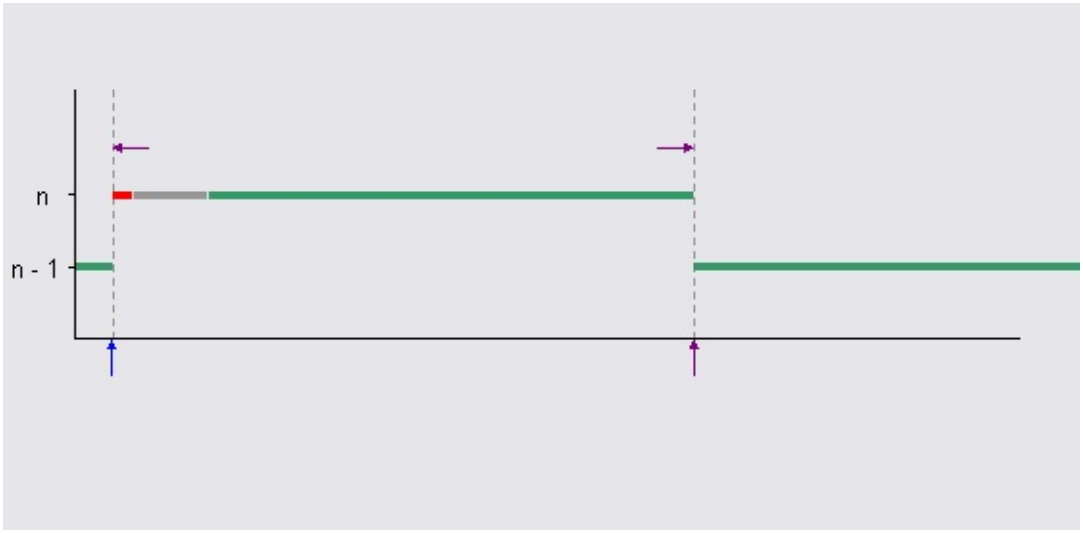
Security Platform

Security
Platform .



Security Platform .
Security Platform .

.

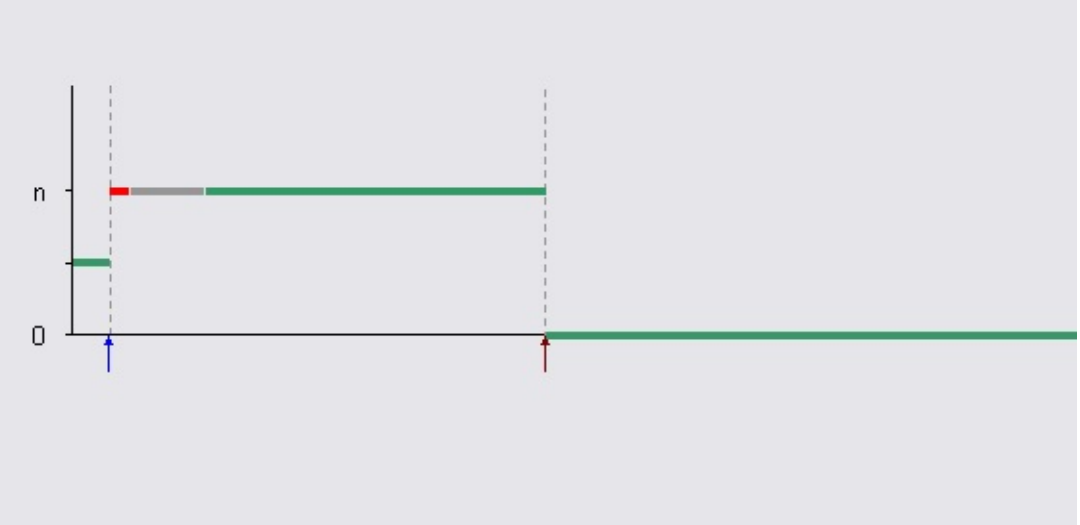

n
n - 1

( ) .
( ). .
.

:

- .
- .
- .

T Security Platform .



, ( ) ( )
. Security Platform
.

Infineon Trusted Platform Module
. Trusted Platform Module .

(: Security Platform)	5	6 5 (_____ _____ _____).
Security Platform	3	6 3 (_____ _____ _____).
(: PIN Windows BitLocker)	10	6 10 (_____ _____ _____).
	~10 s	10.
	~24 h	24. 15 .
	~6 h	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 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) • (: PIN Windows BitLocker) Security Platform . Trusted Computing Group(TCG) Trusted Platform Module . 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 .

. Security Platform

.

1.	: : . : . : (: Security Platform) (: PIN Windows BitLocker) . : • : Trusted Platform Module (_____, " "). • : . • : . . , (_____). : "F5" . : 0 . 0 . Trusted Platform Module .
2. Security Platform	. .< . . . .

Infineon Security Platform

Infineon Security Platform

__ Security Platform .

Infineon Security Platform :

Security Platform	
Security Platform ___	• Trusted Platform Module . • . . Infineon Security Platform .
Security Platform _____	• Infineon Security Platform ( ).
Security Platform _____	• Infineon Security Platform ( ).
Security Platform _____	• Infineon Security Platform ( ).
Security Platform _____	• Infineon Security Platform Infineon Security Platform .
Security Platform _____	• Security Platform .
Security Platform _____	• .
Security Platform PKCS #12	• Personal Information Exchange Security Platform .
Security Platform _____	• .
Security Platform _____	• Security Platform .

Security Platform	• Infineon Security Platform .
Security Platform	• Trusted Platform Module .
Security Platform	• Trusted Computing Group (TCG) .

Infineon Security Platform

Security Platform

Security Platform Infineon Security Platform

. .

. .
.
.

.

.

. .

. ( ) .

Security Platform

.

: Security Platform (Platform)
( ).

Security Platform

. _____

.

Security Platform . .

Windows **Windows**	**Security Platform /Security Platform ( ):** Windows . (, .) Trusted Platform Module .
Security Platform	Security Platform ____ ____ .
	, PKCS #12 : Security Platform .
Security Platform **Trusted Platform Module**	**Security Platform /Security Platform ( ):** . • Security Platform Infineon Security Platform . • Trusted Platform Module Infineon Security Platform . **:** Trusted Platform Module . . • Trusted Platform Module • Trusted Platform Module • Infineon Security Platform .
	: Security Platform . . • .

	• .

Infineon Technologies AG

Infineon Security Platform

Security Platform Security Platform .

.

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

.

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

Security Platform

Security Platform (:)

.

	.
	Security Platform .
...	Security Platform .
	.
	.
	.
	Security Platform .
...	Security Platform .
USB	
PIN	USB . PIN .
	.
 PIN	Security Platform .
...	Security Platform .

	(:).  .
	.
	Security Platform .
...	Security Platform .

Security Platform

Security Platform .

(,)

	. .
	.
USB	
	. .
	.
PIN	USB . PIN .
	. .
	.
	(:). .

	.
	. .
	.

USB	
PIN	USB . PIN .
	. .
	.
	. .
	.
	(:). .

(, /,)

	.
	.
	.
	.
USB	
PIN	USB . PIN .

	(:).  .

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 . Security Platform
  Windows . Windows
  EFS PSD
  Security Platform .
- . .
  . ,
  .
- .
- .
- . .
  .
- .

:

	: • (***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 .

:

	• Infineon Security Platform
__	• • Security Platform • Security Platform • Security Platform
	• ( ) • •  __ Trusted Computing Management Server . PSD(Personal Secure Drive) .
	• Security Platform • Security Platform  __ Trusted Computing Management Server . , .
__	• ( ) • • ( ) •  __ Trusted Computing Management Server . , . .
BitLocker	• Trusted Platform Module BitLocker

	.  • BitLocker (: Windows 7 Windows Vista Enterprise Ultimate editions) . • __ . Microsoft BitLocker BitLocker .
	• • Security Platform • Security Platform / • Security Platform •  • . • __ Trusted Computing Management Server Security Platform .

- **Security Platform**

_____ .

(: Windows 7 Windows Vista)

.

- **Security Platform**

_____ .

(: Windows 7 Windows Vista)

.

Infineon Security Platform -

Infineon Security Platform

Infineon Security Platform .
Infineon Security Platform .

.

abc *Security Platform*	Security Platform __.
abc *Security Platform*	Security Platform , , .
abc *Trusted Platform Module*	Trusted Platform Module
	Trusted Platform Module . .
...	Infineon Security Platform .

Infineon Security Platform -

. :

-
-
- Security Platform
-
-

:

...	. . Security Platform (*.txt). .

Infineon Security Platform -

Security Platform

Infineon Security Platform :

(Trusted Platform Module)

Trusted Platform Module . .

- - Infineon Security Platform Trusted Platform Module
  .
- - Trusted Platform Module . BIOS
  Infineon Security Platform .
  : Trusted Platform Module BIOS BIOS .
  Infineon Security Platform Trusted Platform Module
- - Trusted Platform Module .
  .
  : Infineon Security Platform 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 Microsoft TPM(
) Trusted Platform Module . ,
  Trusted Platform Module Infineon Security Platform
  .
  2 : . ,
  .
  Infineon Security Platform . Security
  Platform **(2)** .
  : Security Platform .

. .

- - Infineon Security Platform
  (:).
  : Security Platform Security Platform
  .
- - Infineon Security Platform . ,
  . ( ).
- - Infineon Security Platform Infineon Security
  Platform . Infineon Security
  Platform . Security Platform (
  :
  Security Platform *Security Platform*
  . .
  .).
  .
  .

: **forceinit** .

__ .

.

. .

/ . :

- : . /
  / / . .
- /: 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
  .
- ____ .

.

...	. .
...	. • • (EFS) Personal Secure Drive(PSD) • ____ ____ .
...	Security Platform / / . Infineon Security Platform ___ .
/...	Infineon Security Platform . Infineon Security Platform

	. Security Platform EFS , Personal Secure Drive Trusted Platform Module . Security Platform . 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 . Infineon Security Platform __ .  • . • __ Trusted Computing Management Server . , .
...	Security Platform . , . . . Personal Secure Drive . PSD PSD . Infineon Security Platform __ .  • Infineon Security Platform . • __ Trusted Computing Management Server . , .
...	Security Platform . Personal Secure Drive .

	Infineon Security Platform . • Infineon Security Platform . • PSD(Personal Secure Drive) . PSD(Personal Secure Drive) .
...	Security Platform . Personal Secure Drive (PSD) PSD . Infineon Security Platform . • Infineon Security Platform . • . • PSD(Personal Secure Drive) .
...	. .

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 __ . . . • Infineon Security Platform • Infineon Security Platform • Infineon Security Platform
...	Infineon Security Platform Infineon Security Platform Security Platform . . . • 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 (.). • 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
  . ,
  . .

.

...	. .
...	. .
...	. . .
...	. .

Infineon Security Platform -

BitLocker

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

:

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

BitLocker .

abc ...	BitLocker . : , , , .
...	Microsoft BitLocker .  TPM(Trusted Platform Module) .

Infineon Security Platform -

Infineon Security Platform

Security Platform .

.

Infineon Security Platform __ Infineon Security Platform .

:

- .
- __ .

:

- Windows editions(: Windows Home editions)
  .
- Security Platform .

.

...	Security Platform . (• Infineon Security Platform . • __ Trust Domain Security Platform .
...	. • ( ) • • • Infineon Security Platform __ . • Infineon Security Platform . • __ Trusted Computing Management Server

	. • _____ Infineon Trusted Platform Module 1.2 Security Platform .
/...	Security Platform . Infineon Security Platform . . **Security Platform :** Security Platform EFS , Personal Secure Drive Trusted Platform Module . Security Platform . 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). • BIOS Infineon Security Platform . • Infineon Security Platform . • __ Trusted Platform Module / .
...	. Security Platform *SpTPMWz.exe* - *resetattack* . • Trusted Platform Module 1.2 Security Platform . • __ Trusted Platform Module / .
...	. . Infineon Security Platform ____ .

	• Windows editions(: Windows Home editions) . • __ . Trusted Computing Management Server .
...	. Infineon Security Platform ____ . • Windows Home editions . • __ . Trusted Computing Management Server .

Infineon Security Platform -

.

:

- .
- __ Trusted Computing Management Server

.

__ .

.

xxx	. . __ .
...	.
xxx	. .
	. _____ . .
xxx	( ).
...	. .
...	. .
	.

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 .
- .
- *Management provider* (,). Security Platform .
- *Management provider* (,). .
- Trust Domain Security Platform .

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

Trusted Platform (Platform Module).

Trusted Platform ( ).

Security Platform :

Security Platform .

Security Platform EFS PSD :

Security Platform .

Infineon Security Platform -

.

.

.

(: USB) .

. .

.

Security Platform .

Security Platform .

, .

BitLocker (: USB) Personal Secure Drive(PSD) .

Infineon Security Platform -

Security Platform .

:

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

Security Platform .

(EFS)	EFS Microsoft NTFS . EFS . Security Platform Solution Trusted Platform Module EFS EFS . EFS , *Documents\Encrypted Data* *My Documents\Encrypted Data* ( ), . EFS
Personal Secure Drive(PSD)	PSD . . PSD . PSD PSD . PSD . PSD . PSD PSD . PSD ( ) *Personal Secure Drive* *Security Platform* . PSD
	Security Platform .

EFS PSD ?

EFS PSD . , .

	EFS	PSD
	, , .	, , .
	Windows Home editions Security Platform Solution .	Security Platform Solution .
	. . EFS . , NTFS .	( ) . PSD . , NTFS .
	EFS .	• EFS : EFS . • EFS : PSD .
	.	, .
	, NTFS .	.
	.	Security Platform Solution .
EFS PSD	(: *My Documents*) .	• Windows Home edition EFS . • . Personal Secure Drive . .

		• FAT32 .

Infineon Technologies AG

Infineon Security Platform -

.

. , Security Platform

.

	Security Platform . , PSD .

Infineon Security Platform -

. .

... .

. . , (:
USB)
. .

Infineon Security Platform -

.

...	. .
...	. . (*SpProtocol_<PCName>_<UserName>.txt*) (*SpProtocol_<PCName>_<UserName>.<DomainName>.txt*). .
	. . (: USB) .

	. . , (: USB) .

Infineon Security Platform -

.

	(: USB) . . .

. USB HD
(: USB) (HD)
.

(USB, HD)	Security Platform .	. .	(USB) : *SpOwner_<PC>.tpm* <*PC*> . (: USB) . USB (: USB).
/ (HD)	/ .	. (: USB) .	/ (USB, HD) : *SpToken_<PC>.xml* <*PC*> (: USB) .
(USB, HD)	.	.	(USB) : *SpPwdResetSecret_<PC>_<User>.xml* <*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	*BitLocker* . *BitLocker* , , .  • BitLocker (: Windows 7 Windows Vista Enterprise Ultimate edition) . • __ . Microsoft BitLocker BitLocker .
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

TPM(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		. Trusted Platform Module .
Trusted Platform Module 1.2 PPI		. Trusted Platform Module .
Trusted Platform Module 1.2 PPI		Trusted Platform Module *Physical Presence Interface* . . Trusted Platform Module

		. .
(: Trusted Platform Module 1.1 / PPI)		BIOS Trusted Platform Module .

:

.

.

Infineon Security Platform -

Security Platform

Security Platform .

	__ Trust Domain Security Platform . , .

Security Platform	Security Platform . .
Security Platform	, Trusted Platform Module , Security Platform . Security Platform Security Platform .

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 (SRK) . Trusted Platform Module Security Platform . Trusted Platform Module SRK SRK .

.

	. . __ .
	( ).
	. _____ . .
...	. .
...	. .

☑	.

. TPM Infineon Technologies AG

Infineon Security Platform -

Security Platform __ .

Security Platform Security Platform __ _____ _____ .

:

- Microsoft , Trusted Platform Module (TPM) Management .
- Security Platform .
- Security Platform OS .
- OS Security Platform BIOS OS Security Platform .

.

__ Trust Domain Security Platform
. , .

TPM Infineon Technologies AG

Infineon Security Platform -

Security Platform

Security Platform (:).

	__ Security Platform , , Trusted Computing Management Server . *BitLocker* Microsoft .

Security Platform .

☑ ( )	Security Platform . . .  _____ .
☑	. . .  _____ . . .
☑ *BitLocker*	TPM(Trusted Platform Module) BitLocker .  BitLocker (: Windows 7 Windows Vista Enterprise Ultimate edition) .
☑	.  . Security Platform .
☑	. _____ .

	_____ Infineon Trusted Platform Module 1.2 Security Platform . Security Platform . ///unstranslated ///unstranslated

Infineon Technologies AG

Infineon Security Platform -

Security Platform . Security Platform

.

	Trusted Computing Management Server . , .

.

: ...	Security Platform . . XML , : SPSystemBackup.xml SPSystemBackup . *.xml .
...	. . PC . "" " " .

Infineon Security Platform -

Security Platform .

:

- Security Platform .
- Trusted Computing Management Server

. , .

__ .

.

	. . .
	. . , .
abc ...	. . XML . : . . . CD .
xxx	. . . __ . . . .
xxx	. .

Infineon Security Platform -

.

:

- .
- __ Trusted Computing Management Server

.

.

.

	. . .
	. . .
abc ...	. . XML .  : . . . CD .
xxx	. . . .
xxx	. .

Infineon Security Platform -

BitLocker

TPM (Trusted Platform Module) BitLocker
.

:

- BitLocker (: Windows 7 Windows Vista
  Enterprise Ultimate edition) .
- BitLocker , ,
  .
- BitLocker BitLocker "
  . BitLocker .
- __ .

.

	Microsoft BitLocker .

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 . Security Platform .  Security Platform . .
2. ____	Security Platform
3. _____	Security Platform
4. Security Platform ___	, EFS PSD ,
5. __	(EFS PSD)
6. _____	
7. __	(EFS PSD)
8. Personal Secure Drive	*Personal Secure Drive*

: **Security Platform**
. . . Security Platform
.

: .

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

: Windows Security Platform
SpUserWz.exe . .

-forceinit */forceinit*	.  . .  . • . • 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 -

(:)

.

:

.

.

☑	.  . .
abc ...	. .  . .

Infineon Security Platform -

(1)

.

.

: .

.

.

.

: , .

Infineon Technologies AG

Infineon Security Platform -

Security Platform

Security Platform .

	: . : ____ .

Security Platform .

☑	. . (__). ____. . .
☑ -	__ . . . EFS PSD . EFS PSD .
☑ - *(EFS)*	Microsoft (EFS) ___ . . EFS . EFS Windows Home editions .
☑ - *Personal Secure Drive(PSD)*	Personal Secure Drive EFS . EFS , PSD Security Platform Solution . . . . PSD UNC . . Personal Secure Drive .

☑	. .

: . , .

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

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 .

.

.

: .

Infineon Technologies AG

Infineon Security Platform -

EFS PSD .
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 .

.

☑ *EFS*	*Documents\Encrypted Data* *My Documents\Encrypted Data* ( ) . (desktop.ini FAT32).
☑	*EFS* . ( ).
...	Security Platform EFS (Microsoft EFS) . Microsoft EFS . • EFS . EFS Security Platform EFS , . Microsoft EFS . • Microsoft EFS (Security Platform). : EFS EFS . EFS .

Infineon Security Platform

Personal Secure Drive

Personal Secure Drive Personal Secure Drive
Personal Secure Drive Personal Secure Drive .
Personal Secure Drive ____ . *Personal Secure Drive(PSD)*
.

Personal Secure Drive .

	/
PSD	**1.** Personal Secure Drives **2.** Personal Secure Drive
PSD	**1.** Personal Secure Drives **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
.

.

Personal Secure Drive	Personal Secure Drive (Personal Secure Driv
Personal Secure Drive	. 32 . , "My Secure Drive" .
Personal Secure Drive	PSD .
	PSD . .

Infineon Security Platform

Personal Secure Drive

Personal Secure Drive .
. Personal Secure Drive
.

.

	(MB) . (: USB) . Personal Secure Drive . Personal Secure Drive . __ PSD PSD (Personal Secure Drive). .
PSD .	PSD . Personal Secure Drive .

PSD

Personal Secure Drive . .

.
, . , PSD
PSD .

PSD .

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

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 .

.

Personal Secure Drive	Personal Secure Drive . "F5" . Personal Secure Drive Personal Secure Drive .
PSD	Personal Secure Drive (: , , PSD) . Personal Secure Drive .
PSD	Personal Secure Drive . Personal Secure Drive .
PSD	Personal Secure Drive . PSD .

Infineon Security Platform

Personal Secure Drive

Personal Secure Drive , PSD
.

.

Personal Secure Drive	Personal Secure Drive (Personal Secure Driv
Personal Secure Drive	. 32 . , "My Secure Drive" .
Personal Secure Drive	PSD .
	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. _ ?_____	Security Platform Security Platform .
2. __	( ).
3. _____ _____	.
4. _____	.

. - - ... - - ...

.

.


TPM

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 Security Platform -

.

.

	__ Trusted Computing Management Server .

abc ...	. .  XML .

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 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) .

	_____	.
	PSD _____	Personal Secure Drive .
	_____	Personal Secure Drive .
	__ __	. Personal Secure Drive .
	_____	, , . Personal Secure Drive .
	__	, . Personal Secure Drive .
	__	, . Personal Secure Drive .
	PSD _____	Personal Secure Drive .

Security Platform

.

: . - - ...

: . - - ...

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

: Security Platform (: Security Platform).

Infineon Security Platform -

.

◉	, Infineon Security Platform . . . ____ PSD(Personal Secure Drive) .
◉	Infineon Security Platform . . __ PSD(Personal Secure Drive) .
◉	Infineon Security Platform . . . , . • . • __ Trusted Computing Management Server .

Infineon Security Platform -

.

	__ Trusted Computing Management Server .

.

abc ...	Security Platform . . XML .

Infineon Security Platform -

Personal Secure Drive

Personal Secure Drive . PSD PSD

.

.

Personal Secure Drive ...	Personal Secure Drive . ... . Personal Secure Drive .
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 . • : 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 Technologies AG

Infineon Security Platform -

Personal Secure Drive

Personal Secure Drive . PSD PSD
PSD .

.

Personal Secure Drive	Personal Secure Drive PSD . PSD . . Personal Secure Drive .
Personal Secure Drive	Personal Secure Drive . . . • 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 . : • PSD . • PSD . • PSD . PSD .

Infineon Security Platform -

/Personal Secure Drive

Personal Secure Drive Personal Secure Drive . .

:

abc ...	.	PSD . .	
	PSD .	. .	
	Personal Secure Drive (Personal Drive).	. .	
abc	. 32 . , "My Secure Drive" .		
	PSD .		
	PSD . .		

Infineon Security Platform -

.

:

- .
- __ Trusted Computing Management Server
  .

.

abc : / *ID*	ID . . ID .
abc : / *ID*	ID .

Infineon Security Platform -

.

:

- .
- __ Trusted Computing Management Server
  .

.

: / *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 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 : -

Infineon Technologies AG

Infineon Security Platform -

.

. .	. . __ Trusted Computing Management Server .
( )	.

Security Platform .

TPM Infineon Technologies AG

Infineon Security Platform -

.

: __ Trusted Computing Management Server .	

	Security Platform (_____ ____). .

.

Infineon Security Platform -

.

: __ Trusted Computing Management Server
.

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

.

Infineon Security Platform -

.

: __ Trusted Computing Management Server
.

abc	. .
...	. . ( ), (:). .
abc	. . .

. .
. .
.

Infineon Security Platform -

. , " "
" " .

abc	( ) ( ).
...	.
	.  .
	: . .
abc	Security Platform . .
...	. .
...	. .  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: *Security Platform PKCS #12*
PKCS #12 . Trusted Platform Module .
.

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 .
xxx	PKCS #12 . .

Infineon Security Platform - PKCS #12

PKCS #12 .

abc	PKCS #12 (: *Personal*). .
...	. . CA *Personal* *Trust* *Root Certification Authorities* . **:** *Personal* .
☑ *PKCS #12*	PKCS #12 . (CA) . (PKCS #12). CA . **:** , CA CA PKCS #12 . *Personal* . → *Personal* . → CA *Intermediate Certification Authorities* . → CA *Trusted Root Certification Authorities* .
☑	. .

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 . .
	.

Infineon Security Platform -

Infineon Security Platform

.

Infineon Security Platform

. .

	____ (: Windows 7 Windows Vista) .

.

Security Platform	Infineon Security Platform __ . .
Security Platform	Infineon Security Platform ____ . Infineon Security Platform . (Security Platform). __ Trust Domain Security Platform .
Security Platform	Infineon Security Platform ____ . Infineon Security Platform . Security Platform . (.) __ .
Security Platform	. Security Platform . Security Platform . __ Trusted Computing Management Server

	.
	. Security Platform .
Personal Secure Drive - *Personal Secure Drive - < : > -*	Personal Secure Drive . PSD (< : >). PSD ( ) .
Personal Secure Drive - *Personal Secure Drive - < : > -*	Personal Secure Drive . PSD (< : >). PSD ( ) .
Personal Secure Drive - *Personal Secure Drive - < : > -*	Windows PSD . PSD (< : >). PSD . /. PSD .
Personal Secure Drive - /	Personal Secure Drive .
Personal Secure Drive -	Personal Secure Drive .

(EFS)	. , EFS . EFS .
	. . . _____.
	Security Platform . Security Platform . : • . • Security Platform Security Platform .
	Security Platform . PSD EFS . : • EFS PSD . *EFS* *PSD PSD* *(EFS)* . • PSD (:).
	Infineon Security Platform . Security Platform EFS , Personal Secure Drive Trusted Platform Module . Security Platform . Security Platform . Trusted Platform Module 1.2 Security Platform .
Security Platform	Security Platform (Security Platform). Security Platform . 1.2 Trusted Platform Module Security Platform . .

	__ Trust Domain Security Platform .
Security Platform	Security Platform . Security Platform . __ Trusted Computing Management Server .
Security Platform	. , Security Platform . __ Trusted Computing Management Server .
/ -	Trusted Computing Management Server . (, " /"). __ . Trusted Computing Management Server . . : • . • Trusted Computing Management Server . • . (, " /"). . . . ____ .

/ -	Trusted Computing Management Server . .  __ . . : • . • Trusted Computing Management Server . • (, " / "). .
/ -	. .  __ . . : • . • Trusted Computing Management Server . • (, " / "). .
	.  __ . : • . • Trusted Computing Management Server . .

	.
	. .  .
Infineon TPM Strong Cryptographic Provider	Infineon TPM Strong Cryptographic Provider . .
	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 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 ... (__).
Security Platform .

Security Platform ____( ) __ ____(
) Security Platform .

Infineon Security Platform -

Security Platform

Infineon Security Platform

.

_____ ____	
_____ ____	
	__ Trusted Computing Management Server .

- .
- Windows Home editions

.

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)
   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 .

.

TPM	: Trusted Platform Module (PPI) Module . . : Trusted Platform Module .	Trusted Pla
	: . : . Trusted Computing Group(TCG) . Security Platform . . . Security Platform .	
TPM *NV*	Trusted Platform Module 1.2 (NV) . NV . : NV , , . : NV . Trusted Platform Module 1.2 Security Platform . Security Platform .	/

	Trusted Platform Module . : (: Security Platform) (: PIN Windows BitLocker) . : . . Infineon Trusted Platform Module 1.2 Security Platform . Security Platform . . ( ). . Security Platform . (:).	: 3 : 5 : 10
	: . : . , .	
	: (S3) (S4) Security Platform . . Security Platform . : Security Platform .	
	: ID(CLSID) CLSID .	.

	. ID . ClassID : {76D8D888-B5AC-49FC-9408-8A45D37F3AC6}. **:** . .	
	: . . **:** .  . .	
SRK	Trusted Platform Module Storage Root Key(SRK) . SRK Security Platform . **:** SRK . **:** SRK .  _____ . . .	

.

-	: (: . : 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 Security Platform . : .	**/Managem Provider**
	: Security Platform ( ). Security Platform . : . Security Platform - -	

: (: \\BackupServer\SecurityPlatformShare\SPSystemBackup.xml).
. XML
, : SPSystemBackup.xml SPSystemBackup .
.

 Security Platform PC .
.

: .

: Security Platform
.

 : . ,
.

: Security Platform
.
.

: (: \\ServerName\FolderName\FileName.xml).
.
Security Platform PC PC
.

 Security Platform PC .
.

: .

_____
? _____

: Security Platform .
Security Platform
.

: . Security Platform
- - ... . .

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

.

Security Platform PC PC

.

 Security Platform PC .

.

:

.

_____

?_____

.

	Security Platform . Security Platform . . .	---
URL	__ .	

Infineon Security Platform -

Infineon Security Platform

Infineon Security Platform .

	__ Trusted Computing Management Server . Trusted Computing Management Server .
	: (,) Security Platform .

.

-	: (: . : 6. _____	, 6
-	: . : . _____	
-	( ) . : • : (: 42). • : (: 7). : . , .	
-	: (: . : 20. . _____	, 20
-	: . : . .	

	_____ _____	
	/: Security Platform . **/:** . , (EFS, PSD) . **:** . Security Platform .	/
Security Platform	**:** Infineon Security Platform Security Platform . **:** Infineon Security Platform Security Platform .  Infineon Trusted Platform Module 1.1 Security Platform . Security Platform .	
	: Security Platform . **:** .	
EFS	**:** Security Platform *(EFS)* . **:** .  EFS Windows Home editions .	
PSD	**:** Security Platform *Personal Secure Drive(PSD)* . **:** .	
	: .	

	Security Platform . : . -	
	: Security Platform ( ). : Security Platform ( ) ( ) .  . Security Platform . 	
	: Infineon Security Platform . . . : .	
URL	: Security Platform . Security Platform . : Infineon Security Platform . : • Security Platform . • : . • EFS (*EFS*).	Infineon
EFS	: EFS . EFS .	

	1. **EFS :** (,) . . • : . • : . • : PC . 2. **URL:** EFS CA (: https://www.companyname.com/foldername). (CA) EFS . • URL . • EFS . • EFS Security Platform PC . EFS . **:** EFS . EFS ., EFS . **:** • EFS EFS PSD . • EFS (EFS PSD) (*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 . : 5000 MB . Windows 7 Windows Vista PSD 20 MB 10 MB. • PSD 5050 MB PSD 50 MB . • 5000 MB PSD .	5000 MB .
	: Security Platform Security Platform . _____ . **:** Security Platform Security Platform .	
MS-CAPI	**:** MS-CAPI . . **:** . . .	
	/ : Infineon TPM Strong Cryptographic	/

	Provider . Strong Cryptographic Provider . **/:** . . **:** . , Infineon TPM Strong Cryptographic Provider .	

.

	: (,) Security Platform . (: 2). **:** .	.
	/ : Management Provider , . **/ :** Management Provider . **:** .	**/Management Provider**

Infineon Security Platform

Security Platform

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

.

		API	/()
Infineon TPM Cryptographic Provider(CSP, AES)	. _____ . . , Trusted Platform Module .	Microsoft Crypto-API	• EFS PSD • Outlook Windows Mail/Outlook Express (S/MIME) • Internet Explorer SSL/TLS • Microsoft Internet Explorer • Microsoft Office • Microsoft Crypto-API VPN • Microsoft Crypto-API • Adobe
Infineon TPM RSA and AES Cryptographic Provider(CSP, AES , Windows 2000)			

			Adobe • EAP-TLS
Infineon TPM PKCS #11 Provider ("TPM Cryptoki Token")		PKCS #11 Crypto-API	• Mozilla Thunderbird (S/MIME) • Mozilla Firefox SSL/TLS • Mozilla Firefox • Sun CA • RSA SecurID • PKCS #11
Infineon TPM Strong Cryptographic Provider(AES)	. __ . . , Trusted Platform Module .	Microsoft Crypto-API	• VPN .
Infineon TPM Platform Cryptographic Provider(Platform CSP)	. Trusted Platform Module	Microsoft Crypto-API	• WLAN WLAN RADIUS IEEE

	. . , Trusted Platform Module . CSP .		802.11 EAP-TLS (TLS) • RADIUS LAN IEEE 802.1X EAP-TLS (TLS) • VPN IPSec
Infineon TPM Key Storage Provider(KSP)	Key Storage Provider. Infineon TPM Cryptographic Service Provider . , TPM RSA .	Microsoft Cryptography Next Generation(CNG) API API	• Microsoft .NET 3.0 • Cryptographic Service Provider .

.

Infineon Security Platform

Security Platform

Security Platform Trusted Computing Group(TCG) .

TCG (TSS) .

- TSS(TCG) Service Provider
- TSS
- TSS

TCG TCG , .

:
Trusted Platform Module
 .

Infineon Technologies AG

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 Service .

Client Side Control Agent	Trusted Computing Management Server (____).

Infineon TPM Professional Package Server Integration Services
.

Server Integration Services *ReadmeServerIntegrationServices.t*
. __ Client Side Control Agent .

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 .
(CA) (PKI) .

Security Platform / .

PKI
.

Windows (PKI)

PKCS #11

Infineon Security Platform Solution

ID ID

.

.

-
-
-
-
- CA
- CA

.

-
- ( )
- (: , ,)

(Certificate Authority: CA) 3
. CA . .

.

Infineon Security Platform

CA

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

CA .

-
-
-

CA . CA CA
Certificate Practices Statement(CPS) . CA CA
CPS .

CA .

- CA ?
- CA? CA . CA
  .
- CA ?
- CA ?
  , .
- CA ?

CA CA . CA .

	Security Platform ____ .

.

Infineon Security Platform

Windows (PKI)

Microsoft Windows 2000 Windows (PKI) .

Windows .

. , .

PKI (DC) Kerberos Key Distribution Center(KDC)
Windows . , PKI
.
, ,
, , . Windows 2000 Windows NT 4
.
, .
.

Microsoft PKI Microsoft TechNet .

PKI .

- Active Directory
-
-
-

.

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 .

Infineon Security Platform

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

Windows 2000 , , CA
CA .

Windows 2000 CA . CA
. CA , CA
.

CA Windows 2000 , . , CA
.
.

Windows 2000 CA .
Windows 2000 CA .

: CA .
Active Directory CA . CA Active
Directory DNS .

CA Microsoft TechNet .

PKI Security Platform
_____ .

Infineon Security Platform

Active Directory (CSP)

. Security Platform

.

Active Directory ?

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

2. **ADSI Edit**

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

3.

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

4.

   CN=User .

   : *pKIDefaultCSPs.*

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

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

   :
   3,Infineon TPM Cryptographic Provider

   .

(CA) Security Platform .

: Security Platform ____
Active Directory .

Infineon Technologies AG

Infineon Security Platform

.

.

.

Security Platform

.

- Microsoft
- Microsoft Windows

Infineon Technologies AG

Infineon Security Platform

MMC(Microsoft Management Console)

CA Windows .

1. Microsoft
   Microsoft .

2. ... .

3. .

4. . Security Platform .

   .

5. Security Platform .
   CSP .

   Security Platform
   .

   .

6. .
   .

7. .
   .

8. .

.

Infineon Security Platform

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

CA .

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

2. .

.
Security Platform
.

.

.

CSP:	*MS V1*
:	*CSP*
:	
:	*GUID*

MS V1 .

Security Platform .
CSP GUID.

Security Platform
.

.

.

.

Infineon Security Platform

PKCS #11 (PKI)

PKCS #11 , . PKCS #11
.
. PKCS #11
.

PKCS #11
.

PKCS #11 .
PKCS #11 .

PKI PKCS #11
. PKCS #11
. .
LDAP(Lightweight Directory Access Protocol) .

Windows 2000 / XP PKCS #11 3
. Infineon Security Platform
Trusted Platform Module PKCS #11 .

.
.

PKCS #11 PKCS #11
.

PKCS #11
.
.
.
.

, .
.

PKI .

-
- 3
- Infineon Security Platform PKCS #11 Mozilla Firefox
-

.

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

Infineon Security Platform Solution

Mozilla Firefox PKCS #11

PKCS #11 PKI .
. Infineon Security Platform Infineor
Platform PKCS #11 ( ) .
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. .

Infineon Security Platform

.
.
.

Security Platform ____

.

- Sun __
- PKCS #11 CA ____

Infineon Technologies AG

Infineon Security Platform Solution

Sun

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

PKCS #11 .

Mozilla Firefox

1. Mozilla Firefox .
2. Mozilla Firefox .
3. . .
   1025 SSL
   . *https://your_server_name:1025*.
4. .
5. . .
   - .
   - .
   - .

: .

:

1. > ... .
2. .
3. .
   - .
   - /
     .
   - .

Infineon Security Platform

PKCS #11 CA

CA .

. Sun . . CA

.

.

Infineon Technologies AG

Infineon Security Platform

Personal Secure Drive

Personal Secure Drive(PSD) . ____
Personal Secure Drive .

Personal Secure Drive . , Personal Secure Drive
. Personal Secure
Drive .

Personal Secure Drive .

1.
2.

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

:
PSD .
PSD
.

PSD Trusted Computing Management Server . , PSD
(____).

PSD .

(: USB) PSD . PSD .

(:) PSD PSD
PSD (Securi
). PSD .

Infineon Security Platform Solution

Personal Secure Drive

. Personal Secure Drive

. Personal Secure Drive :

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

Personal Secure Drive

. Personal Secure Drive :

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

Trusted Platform Module

Personal Secure Drive (**Trusted Platform Module(TPM)**
. Personal Secure Drive
PC "" .
Module .

Personal Secure Drive

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

Infineon Security Platform - PSD PSD

Personal Secure Drive

Personal Secure Drive () ()

.

PSD . PSD . PSD PSD

.

PSD

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

Windows Explorer PSD .

PSD

Windows PSD .

_____, **Personal Secure Drive -** (Personal Secure Drive) **Personal Secure Drive - < : > -** (Personal Secure Drive). .

PSD

_____ **Personal Secure Drive -** . PSD (Personal Secure Drive) **Personal Secure Drive - < : > -** Personal Secure Drive).

PSD

PSD Security Platform __ .

PSD

PSD Personal Secure Drive .
PSD .

PSD	
Personal Secure Drives	Personal Secure Drive . . . "F5" .
☑	Personal Secure Drive PSD . PSD .
☐	.
☐	PSD PSD .

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 .

.

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 editions	EFS Windows editions
	• PSD . PSD PSD . • PSD .	• EFS . • Microsoft . • PSD PSD .
:		
PSD	**1.** PSD **2.** PKCS #12 PKCS #12 . : PSDRecovery /R:filename **3.** PSD : : PSDRecovery /A:filename.CER [/ID:driveID] : 2 1 .	**1.** PSD **2.** Microsoft EFS : : secpol.msc **3.** 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] [/ID:driveID]	Microsoft EFS : secpol.msc
PSD **:**	• . (, 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 .

 .

PSDRecovery /A:filename.CER [/ID:driveID] EFS Windows editions .
*.CER Personal Secure Drive .
filename.CER — .CER
/ID:driveID — : ID Personal Secure Drive .
PSDRecovery /D:name [/ID:driveID] **PSDRecovery /D:number [/ID:driveID]** Windows Home editions .
PSD . (PSDRecovery /V) .
name — PSDRecovery /V
number — PSDRecovery /V
/ID Personal Secure Drive .
PSDRecovery /L
Personal Secure Drive ID, . PSD .
PSDRecovery /M:DriveImageFile.FSF [X:]
PSD .
DriveImageFile.FSF — PSDRecovery /L PSD
X — (). .

PSDRecovery /R:filename
Windows Home editions .

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

filename	( ). . .

PSDRecovery /V [/ID:driveID]
Windows Home editions .

PSD . . . ,
.

/ID Personal Secure Drive .

Infineon Security Platform

(EFS)

(EFS) NTFS . NTFS
. EFS ( )
. .
.

.

:

- . .
- EFS Windows Home editions .

Infineon Security Platform

EFS

EFS Microsoft . Microsoft EFS
. Microsoft Windows .
F1 .

- .
  .
- . .
- .
- .
- .
  .
- EFS . TCP/IP (IPSec)
  PPTP .

: EFS Windows Home editions .

Infineon Security Platform

(EFS)

EFS .
EFS .

- NTFS .
  Windows 2000 XP NTFS
  . NTFS .
- FAT .
  FAT .
  . FAT
  ( ).
- .
  Windows EFS .
  .
  — .
- .
  .
  . .
  .

.

- . Microsoft EFS.
- . .
- .

.

- EFS .
- . .

EFS . Microsoft EFS. Microsoft Windows . F1

.

EFS .

: EFS Windows Home editions .

Infineon Security Platform

.

.

.

__ Microsoft Windows Mail/Outlook Mozilla Thunderbird .

Infineon Technologies AG

Infineon Security Platform

Windows Mail/Outlook Express/Outlook

.

- _____
- _____
- _____

Infineon Security Platform

Outlook/Windows Mail/Outlook Express

. , .

:

.

Windows Mail/Outlook Express

Outlook 2007

Outlook 2003

Outlook XP

Outlook 2000

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 Security Platform

Mozilla Thunderbird

Mozilla Thunderbird

.

- _____
- _____
- _____

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 .

Infineon Security Platform

Mozilla Thunderbird

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

. .

Infineon Security Platform

Mozilla Thunderbird

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

Infineon Security Platform Solution

Microsoft Word

Microsoft Word

.

.

Microsoft Word 2000 Microsoft Word XP .

Infineon Security Platform

Microsoft Word

Microsoft Word . .

Microsoft Word ,

. .

Microsoft Word .

.

Infineon Technologies AG

Infineon Security Platform

Microsoft Word

1. >>... .
2. : //.

1. .
2. >> **... .** (Microsoft Word 2007 : > > ...).
3. .
4. .
5. .
6. .

Microsoft Word 2007 ()

1. .
2. > > , . .
3. . .
4. **Visual Basic** . .
5. **Project Explorer** .
6. Visual Basic > **...** .
7. **...** .
8. .
9. .
   : . .
10. .
11. .
12. Word .
    : **Microsoft Word**
    .
13. > Microsoft Word .

()

1. .
2. >> .
3. . , , .
4. **Visual Basic** . .

   : **Visual Basic** >>**Visual Basic Editor** .
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 Provider) Trusted Platform Module
.

.

- / ( )
- (VPN)
- LAN(WLAN) LAN

.

.

	Security Platform		
/ ( )	Infineon TPM Cryptographic Provider Infineon TPM RSA AES Cryptographic Provider (CSP)	SSL/TLS	
/ ( )	Infineon TPM PKCS #11 Provider	SSL/TLS	
VPN	Infineon TPM Cryptographic Provider Infineon TPM RSA AES Cryptographic Provider (CSP)	IPsec	
VPN	Infineon TPM Platform Cryptographic Provider(Platform CSP)	IPsec	
WLAN LAN	Infineon TPM Cryptographic Provider Infineon TPM RSA AES Cryptographic Provider	WLAN: IEEE 802.11 EAP-TLS LAN: IEEE 802.1X EAP-TLS	

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

.

Infineon Security Platform

ID

.

.

.

.

.

ID . ID .

ID .

.

(: SSL)

.

.

. ID
.
.
, .
.
.
.
. IIS Active Directory
Internet Explorer .

- IIS Active Directory
- Internet Explorer

Mozilla Firefox PKCS #11 .

- Mozilla Firefox
- Mozilla Firefox

Infineon Security Platform

Internet Explorer

Internet Explorer

.

Internet Explorer Microsoft TechNet .

Infineon Technologies AG

Infineon Security Platform

IIS Active Directory

Windows 2000 / XP Windows 2000 / XP Active Directory
 Internet Information Services(IIS) .

 IIS Active Directory .
 Active Directory . IIS
.

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

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

Infineon Security Platform Solution

Mozilla Firefox

Mozilla Firefox

.

.

.

.

.

Infineon Technologies AG

Infineon Security Platform Solution

Mozilla Firefox

.

. .

.

. .

: ( ) .

.

: SSL(Secure Sockets Layer) CA

. SSL

.

Infineon Security Platform Solution

(VPN)

VPN ( ) .
VPN "" .

(VPDN) , ' LAN' .
, VPN
(ESP) . ESP (NAS)
.

Infineon Security Platform Solution

(EAP)

(EAP) (Virtual Private Network)
.

EAP VPN . EAP
(VPN) .

EAP (CA) Security Platform . VPI
EAP (X.509) .

Infineon Security Platform

EAP VPN

Infineon Security Platform Solution .

. .

. Trusted Platform Module .

Security Platform ____ .

. .

VPN Microsoft TechNet Microsoft VPN .
Microsoft Windows . F1

.

(VPN) . VPN VPN

.

EAP . VPN

. Microsoft Windows
Microsoft TechNet .

EAP . .

- VPN .
- SmartCard
  (EAP) .
- EAP .

VPN . VPN
Security Platform ____ .

EAP .

Infineon Security Platform

LAN(WLAN)

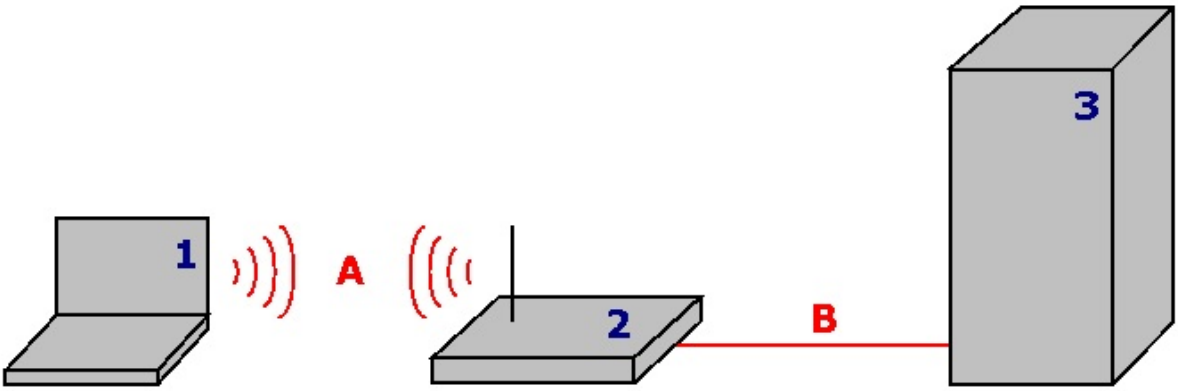
Security Platform WLAN(IEEE 802.11 EAP-TLS) LAN(IEEE 802.1X EAP-TLS) . Security Platform (CSP) .

WLAN .

WLAN

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

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



1	**WLAN**	Security Platform PC. Trusted Platform Module . WLAN (**A**) .
2		"" . WLAN WLAN (**B**) .
3	**RADIUS**	, Microsoft Windows 2003 Server Internet Authentication Service(IAS). RADIUS .

WLAN .

- Microsoft Developer Network(MSDN) Microsoft Windows ("
  ")
- Wi-Fi
- LAN (WLANA)

Security Platform WLAN

:

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

WLAN

Infineon Technologies AG

Infineon Security Platform

WLAN

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

WLAN

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

WLAN . WLAN RADIUS
. .

:
.

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

CSP Administrators .

WLAN

WLAN WLAN . WLAN
.

WLAN .

- Microsoft Windows (" ") WLAN
  .
- .
  - **IEEE 802.1x** .
  - **EAP** .
  - .
  - .

Administrators .

WLAN

WLAN WLAN .

WLAN .

- Microsoft Windows (" ") WLAN .
- " " .

Infineon Security Platform

(FAQ)

(FAQ)

Infineon Technologies AG

Infineon Security Platform

(FAQ)

Infineon Security Platform ?

?

Infineon Security Platform ? ?

?

Internet Explorer . .

. EFS ?

?

EFS . ?

?

Infineon Security Platform ? Infineon Security Platform ?

( )?

?

EFS Windows editions EFS .

Infineon Security Platform ?

.

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

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

:

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

2.0\PlatformKeyData
IFXConfigSys.xml
IFXFeatureSys.xml
TCSps.xml
TPMCPSys.xml

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

:

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

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

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

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

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

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

:
HKEY_LOCAL_MACHINE\SOFTWARE\Infineon\TPM Software
HKEY_CURRENT_USER\Software\Infineon\TPM software

Personal Secure Drive Personal Secure Drive
.
[HKEY_LOCAL_MACHINE\SOFTWARE\Infineon\TPM Software\PSD]
[HKEY_CURRENT_USER\SOFTWARE\Infineon\TPM Software\PSD]

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

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

↑

Internet Explorer . .

Internet Explorer . Internet Explorer
.

↑

. 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

.

?

( ).

:

- (:) ( ) .

.

.

- .

- .

Script GeneratePubKeyArchive.vbs:

```
'GeneratePubKeyArchive.vbs <Full path to Token.xml> <Full path to
PubKeyArchive.xml>
'<Full path to Token.xml>       :
' - SPPwdResetToken.xml
' - SPEmRecToken.xml
' - SPGenericToken.xml
'<Full path to PubKeyArchive.xml>       :
' - SPPwdResetTokenPubKeyArchive.xml
' - SPEmRecTokenPubKeyArchive.xml
' - SPGenericTokenPubKeyArchive.xml
'"       "    :
' - SPEmRecTokenPubKeyArchive.xml
' - SPGenericTokenPubKeyArchive.xml
'"       "    :
' - SPPwdResetTokenPubKeyArchive.xml
' - SPGenericTokenPubKeyArchive.xml
'  ,  :
' GeneratePubKeyArchive.vbs "c:\tmp\SPGenericToken.xml"
"c:\tmp\SPGenericTokenPubKeyArchive.xml"
If WScript.Arguments.Count <> 2 Then
   WScript.Echo ": " & Wscript.ScriptName & " ""<Full path to
Token.xml>"" ""<Full path to PubKeyArchive.xml>"""
   WScript.Quit
End If
Set MPBase = WScript.CreateObject("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 ""
```

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

. ,

?

Infineon Security Platform EFS .

,

EFS . ?

Windows Home editions EFS EFS

.

Trusted Platform Module .

Security Platform Security Platform .

.

. Infineon
Security Platform (" ", 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 , Windows Vista *Trusted Platfc*
(TPM) Management).

↑

Infineon Security Platform ?

Trusted Platform Module
. Security Platform
.

Infineon Security Platform
.

Infineon Security Platform Infineon Security Platform __
.

ID(SID) .
. .

__ 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 .

MMC(Microsoft)

MMC Security Platform Security Platform .

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

, , Security Platform
PKCS #12 .

.

: Security Platform . , Trusted
Platform Module .

: EFS PSD .
(CA) .

EFS :

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

... *EFS* .
EFS EFS PSD .

.

URL .

	. , .  *(EFS)* . EFS PSD .
	PC (:) . .  .  . .  . EFS PSD .
...	.
...	PKCS #12 . Security Platform PKCS #12 . Trusted Platform Module .  _____ .
	.
	Infineon TPM Cryptographic Provider .
PKCS #11	PKCS #11 Security Platform .
	Trusted Platform Module

	. . Microsoft .
	PC . EFS PSD Trusted Platform Module . . .
	.
...	(CA) . . . . *EFS* .
	. Security Platform Microsoft (CA) . CA . : • CA . : CA, . . • *EFS* . CA . • EFS .
	EFS PSD . .

	EFS PSD .

: Security Platform (- - ...).

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

Infineon Security Platform -

.

.

:

.

☑	. . : - - ...