

Details on Security Functions in the Pocket PC 2002 Operating System

Power-On Protection

 **Einstellungen**   20:31 

Kennwort   21:10

 **Einstellungen**   21:36

Kennwort

Besitzer: Henrich C. Poehls

Besitzer: Henrich C. Pöhls

- Kein Kennwort
- Einfaches 4-stelliges Kennwort
- Komplexes alphanumerisches Kennwort

Erforderlich, wenn Gerät nicht benutzt wurde für:

- 1 Stunde
- 0 Minuten
- 1 Minute
- 5 Minuten
- 15 Minuten
- 30 Minuten
- 1 Stunde
- 90 Minuten
- 2 Stunden
- 12 Stunden
- 24 Stunden

Kennwort:

1	2	3	4
4	5	6	7
7	8	9	0
CLR			

Geben Sie Ihr Kennwort ein.

-	-	-	-
1	2	3	4
4	5	6	7
7	8	9	0
CLR			

Geben Sie Ihr Kennwort ein.

*	*	*	*
1	2	3	4
4	5	6	7
7	8	9	0
CLR			

- Pocket PC Phone Edition:

– Emergency Numbers are displayed

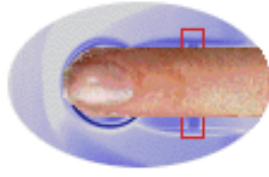
Power-On Protection (2)

- Biometric Signature (in iPAQ 5450)

Settings   00:31 

Training -- Learn by Example

Please follow the demonstration to swipe a finger.



GOAL: 6 out of 8 successful swipes

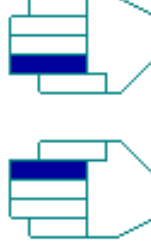
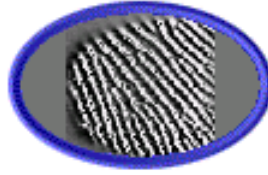


About

Owner Information   00:00 

Owner: Henrich C Poehls

Enter your PIN or swipe one of the enrolled fingers.



Settings   00:01 

Password

PIN OR fingerprint

- No password
- Simple 4 digit PIN
- Strong alphanumeric password
- PIN OR fingerprint**
- PIN AND fingerprint
- Password OR fingerprint
- Password AND fingerprint
- Fingerprint-only

1	2	3
4	5	6
7	8	9
CLR	0	ENTR

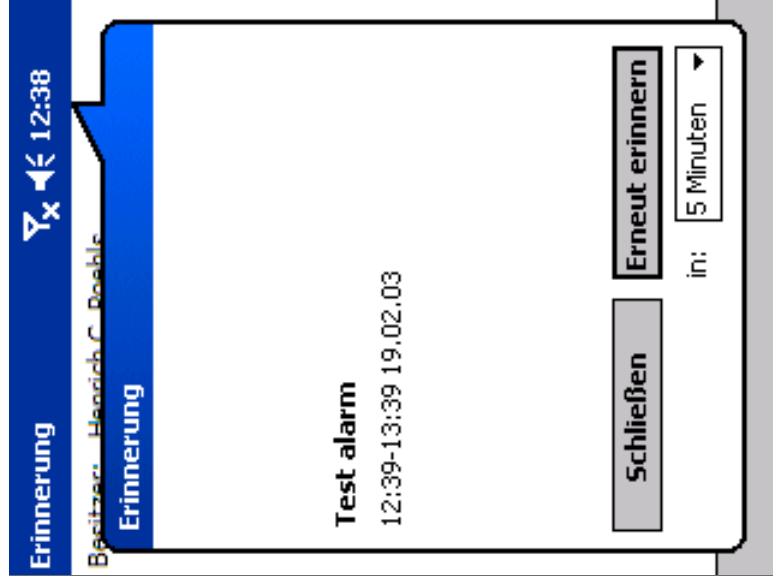
PIN Fingerprint

About

About Options

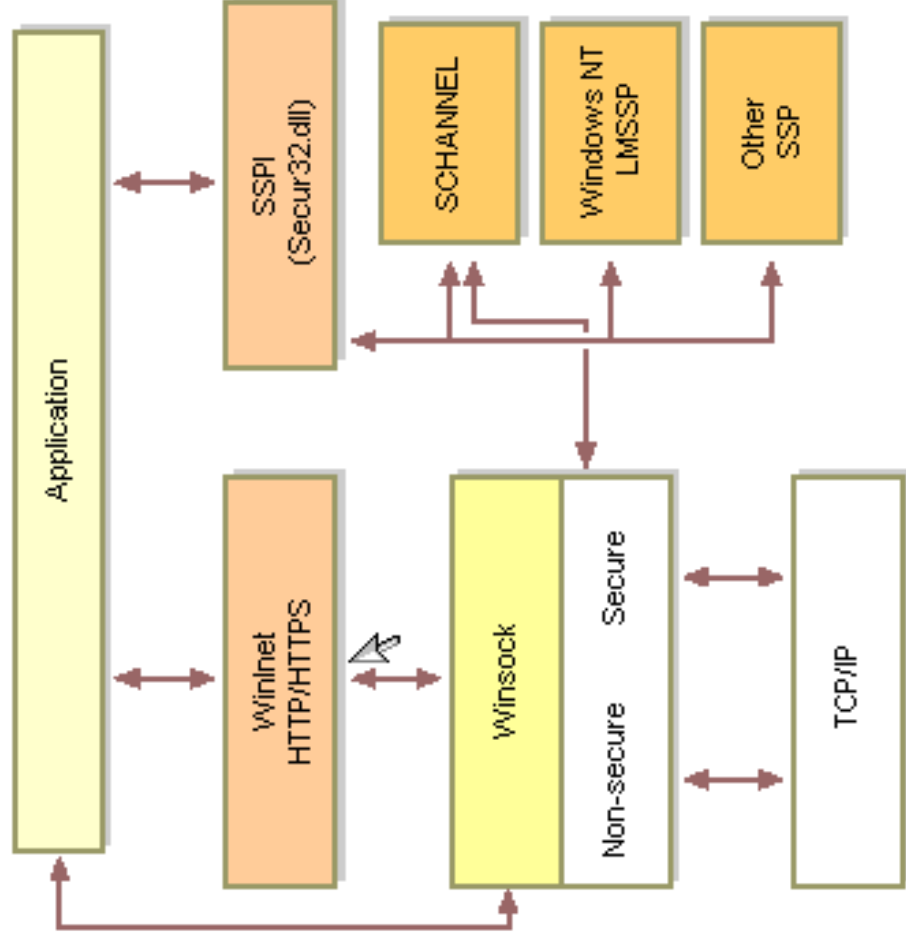
Power-On Protection (3)

- Known Problem:
 - Power-On Protection is enabled
 - Mobile Device goes to sleep
 - An Alarm wakes it up
 - **Alarm info is shown, even device shall be protected !**

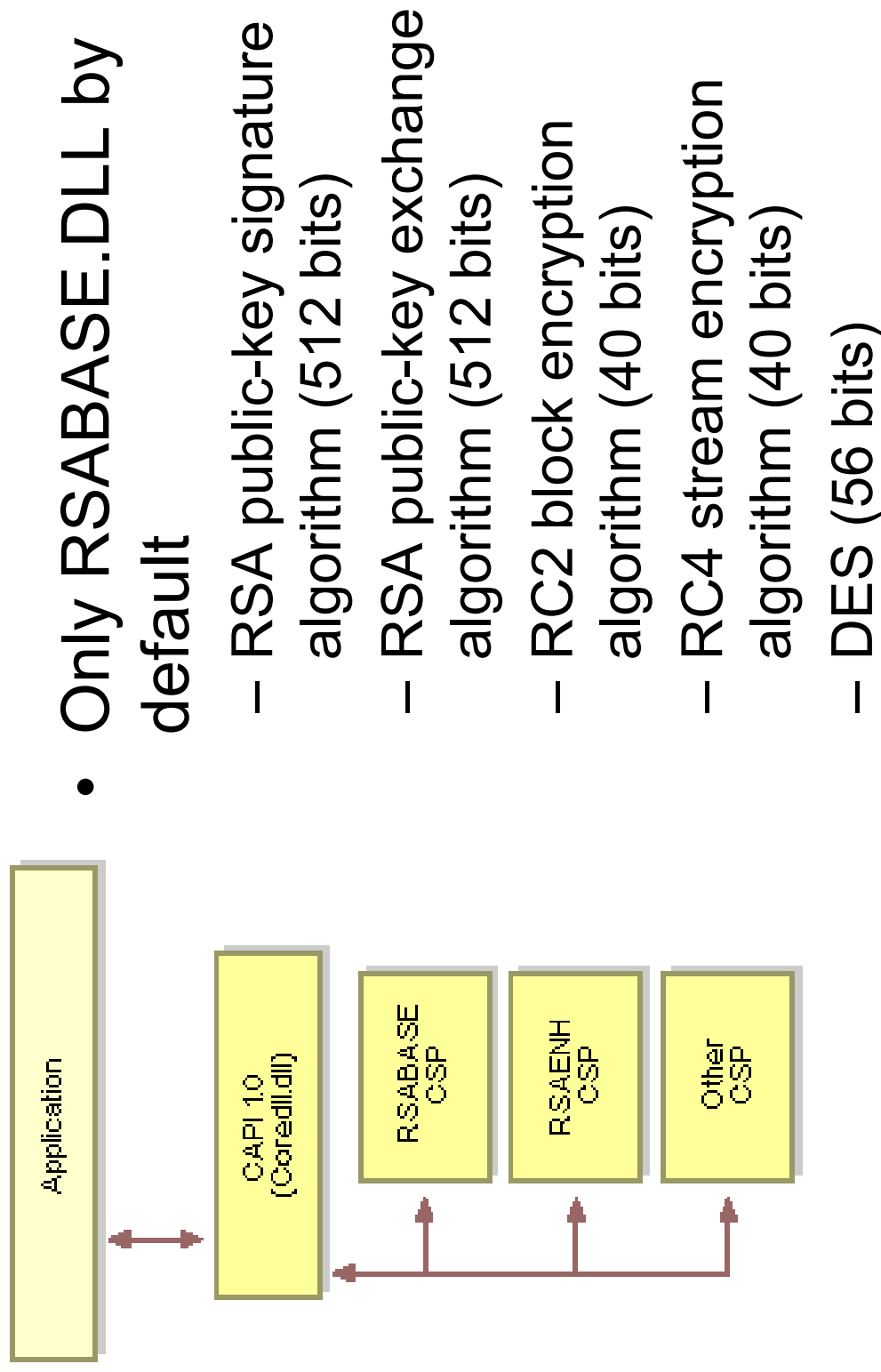


SSPI

- SCHANNEL
 - SSL
 - Certificates
- NT LAN Manager



CAPI

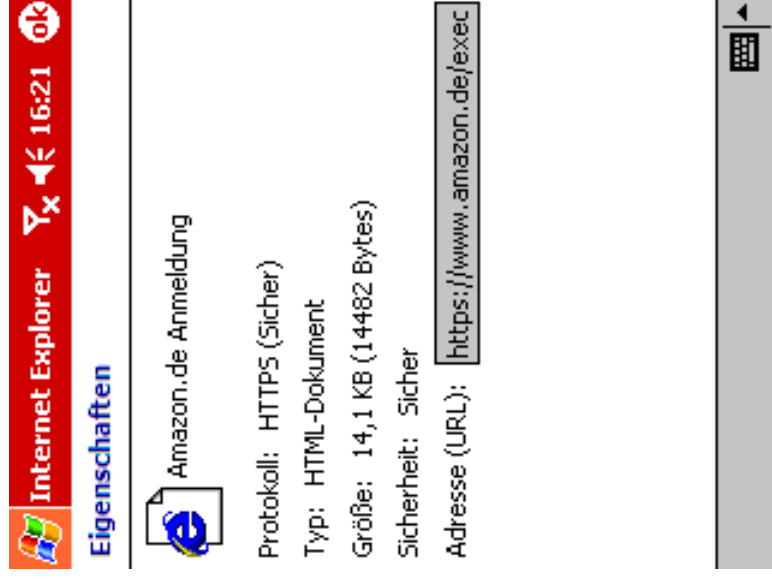
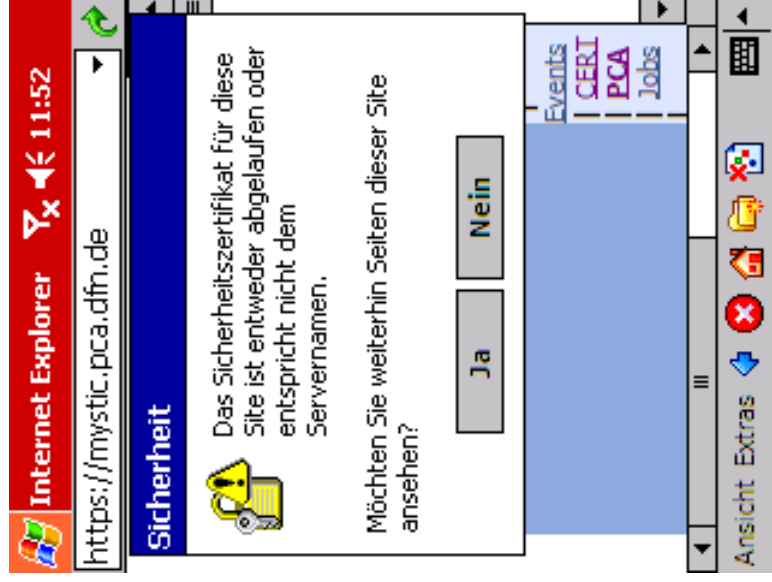


Digital Certificates

- 12 root certificates in the `channel1.dll`
 - Verisign (Class 1, Class 2, Class 3, Class 3)
 - RSA Data Security
 - Cybertrust
 - Thawte (Server CA, Premium Server CA)
 - MS SGC Authority (1024bit, 2048bit)
 - Entrust (1024bit, 2048bit)
- No application to manage certificates

Digital Certificates (2)

- Certificates in PIE (DEMO)



Trust-Model

- Windows CE 3.0 offers a trust model
- not implemented in Pocket PC 2002
- but in Smartphone 2002 (pressure of operators)
- Allows to restrict applications and what applications can do on the Smartphone 2002
- Three levels of trust
 - Privileged trust: Allow full access (normally not granted to applications by the operators)
 - Unprivileged trust: Allow limited access
 - Untrusted (will not load or execute)

Smartphone / CE 3.0 Trust-Model (2)

- Applications are digitally signed normally by the operator
- A Certificate for checking this digital signature is in the Mobile Device
- Level of trust is assigned during signing process and is protected by the digital signature
- Smartphone mobile device is set by default to allow only trusted applications:
 - Privileged trust: Allow full access (not granted to third party applications)
 - Unprivileged trust: Allow limited access

Smartphone / CE 3.0 Trust-Model (3)

- Orange, operator of the only available Smartphone 2002 device has control over the applications that can run on their mobile device
- The developer's and user's where not very happy with this security
- Tools / Manuals how to “unlock” circulated
- Orange recently announced that they will “unlock” the mobile device for development purposes (www.developers.orange.com)

OS in Detail

END