PC/SC Workgroup

MEETING MINUTES
for May 15, 2007, Palace Hotel, San Francisco

MEMBERS PRESENT

Marc Jacquinot	Assa Abloy ITG (Omnikey)	mjacquinot@aaitg.com
Matthias Lochner	Cherry	matthias.lochner@cherry.de
Thomas Zapf	Cherry	thomas.zapf@cherry.de
Jean Lusetti	Gemalto	jean.lusetti@gemalto.com
Jean-Philippe Mailloux	Gemalto	jean-philippe.mailloux@gemalto.com
Eirik Herskedal	Microsoft	eirikh@microsoft.com
Shivaram Mysore	Microsoft	smysore@microsoft.com
Dan Sledz	Microsoft	dsledz@microsoft.com
Calai Bhoopathi	SCM Microsystems	calaib@scmmicro.com
Uli Dreifuerst	PC/SC Administration	admin@pcscworkgroup.com

MINUTES

The meeting began at 7:15 pm.

1. PART 10 REVISIONS

Extended Properties for Scrolling and Display

The Workgroup proposes to migrate from the current ISO 646 (ASCII) standard to support for UTF8. Dan Sledz suggested a new field/parameter, for example, hex 11 (decimal 17), to indicate extended properties in the IFD. Dan will submit a proposal to the group by next week.

The group members will check back with their engineers to identify any backwards compatibility issues. The question is what will break if we change.

Support for Secure PIN Entry (SPE) and FEATURE_WRITE_DISPLAY

Should PC/SC allow Secure PIN Entry and display of arbitrary characters? SPE is typically indicated by a LED or special character. The key problem is the feature GetKey that could be used to intercept a PIN. The more lenient Common Criteria expects the

customer to know if SPE is turned on. The tougher bank standards however do not want to leave decisions about security to the customer. Signed drivers with switching capability were considered too weak, a firmware switch might be acceptable. A concern was raised that with keyboard entry there would always be a suspicion even if a light indicating SPE was on.

Cherry, Gemalto, Omnikey and SCM will continue discussion of this issue via email.

Changes to proposed revision
Dan Sledz will send out a new revision that will address the two comments below:

- p23 : "The IFD must provide for each application ID and for each language ID a storage for up to 254 messages" should be replaced by "the IFD/IFD handler" because according to teleconference minutes from 16 January, strings could also be stored by the driver.

- We think that the existing IFD PIN PROPERTIES structure should not be changed by adding wLcdMaxCharacters and wLcdMaxLines because it will break existing applications. It is better to define a new structure + IOCTL for this kind of information.

2. DEFINITION OF NEW CLASS BYTES, PROPOSAL FROM KOBIL

Since Kobil was not present at the meeting, this topic will be added to the email discussion of part 10.

3. GENERAL AUTHENTICATE COMMAND, HANDLING OF HISTORICAL BYTES

The Workgroup accepted Omnikey's proposal. The Workgroup Administration will send the Word file of Part 3 to Thomas Bruendl. He will return the updated document back to the Administration who will send it out to the group for review.

A question came up concerning use of the CRC after the historical bytes. It was suggested that Omnikey clarifies its use in the next revision of part 3 as follows:

ATR + CRC + Historical Bytes + CRC

4. BIOMETRIC DEVICES

The ISO subcommittee SC37 that defines a biometric hardware interface is expected to have first results available by July. Shivaram will contact Uwe Schnabel from Omnikey and coordinate a proposal to the group.

By providing an abstraction layer and by using a modular approach with clearly defined interfaces between sensors and algorithms, PC/SC could evolve into an "authentication framework" that supports not only smart cards but also biometric devices such as

fingerprint readers, face recognition systems, cameras, etc., and Trusted Platform Modules (TPM).

Discussion of this topic will begin in July with Shivaram's mail to all interested members of the group.

The topic certificate management with biometrics according to IEEE 1667 was dismissed as not relevant in the current market.

5. MULTI-APPLICATION

The group sees no pressing demand for multi-application in the market yet.

Regarding EMV, it was suggested to define an IOCTL to switch a reader from ISO mode to EMV, i.e. EMV class 1 reader. Jean-Phillipe Mailloux from Gemalto will submit a proposal in July.

6. .NET CARDS USE CASES

The Resource Manager should not always power off the smart card when no application is connected (see Gemalto's mail from January 30).
A command "Leave Power Up" was suggested, which leaves the card powered up independent of being connected to the card. Dan Sledz will check feasibility and report back by end of next week.

7. FINANCIAL REPORT, WEB SITE UPDATES

The administration reported an account surplus of approx. $30,000 and invited members to suggest activities that promote the goals of the Workgroup. A detailed financial report will be posted in the member section of the website.

The current revision of all specification documents will be posted in original Word format in the member section as well. The administration will also investigate ways to provide an email archive.

The meeting adjourned at 9:30 pm.

Members: Please review the Meeting Minutes, and inform the Workgroup Administration of any inaccuracies within 10 days of receiving them. When no inaccuracies are found, the Minutes will be viewed as having been accepted by the membership.

Uli Dreifuerst

PC/SC Workgroup Administration
admin@pcscworkgroup.com