Flexible Visual Display Units as Security Enforcing Component for Contactless Smart Card Systems

Markus Ullmann
Federal Office for Information Security
D-53133 Bonn, Germany
markus.ullmann@bsi.bund.de

***Abstract* – Today, one existing class of RFID systems are based on ISO 14443 (Proximity Coupling). This is the standard for RF-interfaces of contactless smart card systems. Contactless RF interfaces of smart cards are very often regarded as less secure than contact based smart cards. This tenor may be changed based on our new approach. Therefore we suggest to establish secure password authenticated wireless channels for contactless smart cards. Preliminary, a separate channel for the transmission of a short time secret (password) is needed. Moreover, we recommend to use an optical channel realized by a flexible display. On the whole, we suggest contactless smart cards with a small visual display unit as security enforcing component to establish a secure and authenticated radio-frequency communication between a contactless smart card and a contactless reader.**

I Introduction

The considered system consists of a reader also referred to as interface device (ifd) and a contactless smart card so called integrated circuit card (icc). A communication with a contact smart cards can only take place if the smart card is inserted into an interface device. Contrary to the widely used contact smart card, contactless smart card communicates with the reader through radio frequency induction technology (at data rates of 106 to 848 kbit/s). These cards require only close proximity to a reader antenna to complete transaction. The standard for contactless smart card systems is ISO/IEC 14443 [2]. The most significant security attack concerning contactless smart cards is that an attacker can communicate with the card without the knowledge of the card holder and even when the card holder carries the card in his pocket. This attack is possible even with passive contactless smart cards. Passive in this context means that the smart card has no electrical power supply (e.g. a battery). From a technical perspective this attack is only possible within a range of less then 25 cm between the attacker's interface device and a contactless ISO 14443 smart card [9].

Nevertheless this is the main security risk which comes up with contactless smart card interfaces. Besides that, an attacker might eavesdrop an existing radio frequency data transmission. A radio frequency communication can easily protected against eavesdropping. Establishing secure channels between two entities is a well known security requirement and there already exist a lot of approaches to deal with it. Most of them use PKI-based cryptographic mechanisms to solve this problem. PKI technologies implies that each reader/interface device must have a certificate. The smart card has to take the validity of the certificate into consideration. One consequence is that every certificate chain of each ifd must be signed with the same root key. Therefore we would have to establish a complex PKI infrastructure. In the context of establishing an authenticated secure radio frequency channel between an ifd and a contactless smart card an PKI approach seems completely inadequate.

There exist already one solution which address the mentioned security problem that an attacker can communicate with the card without the knowledge of the card holder and even when the card holder carries the card in his pocket. This solution was developed in conjunction with the new electronic passport. It's called Basic Access Control protocol. An necessary assumption is that each passport bears an individual electronic cryptographic key. This key is calculable based on personal information of the passport owner which are printed on the data page of the passport. Only subjects or interface devices which are able to read the personal data printed on the passport can calculate the key and access the passport after a successful run of the Basic Access Control protocol. The advantage of this solution is that it's a very practicable one which doesn't imply any investment in a background security infrastructure. But it has some technological founded limitations. Firstly, the individual key is static. And secondly, there exist a correlation between the passport individual key and the keys used for the secret messaging.

So we are looking for an alternative to protect contactless smart cards. The new approach should be as easy and safe to handle as the Basic Access Control protocol. But it should avoid the mentioned limitations. In this approach we suggest to use a password based protocol for the establishment of authenticated radio frequency connections between an ifd and an icc. But the inherent problem of password-based mechanism is the independence between setting up a secure channel and sending the password in a secure manner to the other entity. Password-based cryptographic protocols solve this problem in an elegant way. Those protocols are based on the seminal work of Bellovin and Merret, the Encrypted Key Exchange (EKE) [1]. Besides the first approach of Bellovin and Merret a lot of further password-based cryptographic protocols were published, for example by David P. Jablon [3] or Savan Patel [4]. But it remains always open how to transmit the password before applying the password-based protocol.

The idea to integrate displays into contact based smart card systems comes up a few years ago. We pick up this idea to enhance the security of contactless smart card significantly. Here we propose a new usability of displays in smart card systems as security enforcing device for the establishing of authentic secure radio frequency channels between a contactless smart card system and an interface device (reader) for the first time. This idea is quite new and offers authentication of interface devices in combination with the establishment of secure radio frequency channels. This enormously enhance the trust in contactless smart card systems for those users who carries contactless smart card systems in their pocket. To solve the described security weakness we propose using password-based protocols.

In contrast to the usual deployment of password based protocols with long term secrets we use random short term secrets (passwords) for the authentication of interface devices and the establishment of password authenticated radio channels. The display is needed to handle the short term passwords in combination with password-based protocols. Next we combine the idea of password-based protocols with security mechanism with are used in the context of smart card systems today.

Figure 1 shows the considered system structure in this paper. The considered system consists of a reader and a contactless smart card.

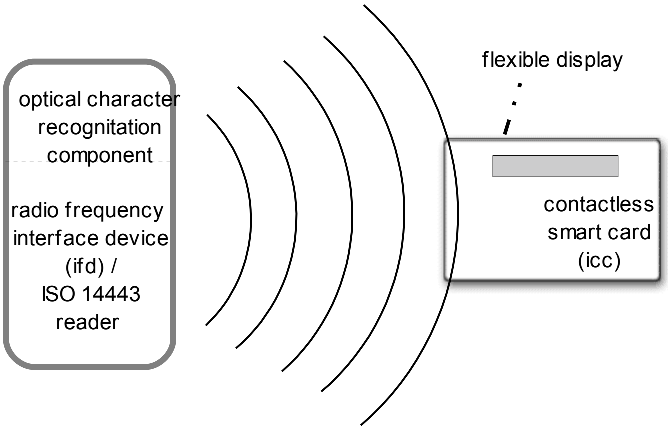
optical character recognitation component
radio frequency interface device (ifd) / ISO 14443 reader
flexible display
contactless smart card (icc)

Figure 1 System Structure

Following notation is used in this paper:

A,B	entities communicating
icc	integrated circuit card and smart card are used as synonyms
ifd	interface device, chip card reader are used as synonyms
r_A, r_B	nonce generated by A / B
n_A, n_B	nonce generated by A / B
K	symmetric key
K_{AB}	a session key shared by A and B
Z_{AB}	a shared symmetric secret key calculated by the entities A and B
$\{M\}_K$	symmetric encryption of message M using the symmetric key K
p	prime
Z_p	the field of integers modulo p
Q	a subset of Z_p
g	a generator of G
G	a subset of Z_p
π	a random short term secret (password)

II Security Requirements for Contactless Smart Card Interfaces

Contactless interfaces of smart cards bear a new security risk. From a security perspective the difference between a contact smart card and a contactless smart card is, that a communication with a contact smart card can only take place if it is inserted into an interface device. Because contactless smart cards communicate with the reader through radio frequency induction technology it is in principle possible that an attacker can communicate with the card without knowledge of the card holder and even when the card holder carries the contactless card in his pocket. This is the main new security risk which comes up with contactless smart card interfaces.

Besides that, there is a further security risk: eavesdropping of the communication between the contactless smart card and the interface device. To avoid the mentioned security risks we define the following security requirements for a secure authenticated connection between a contactless smart card and an interface device:

1. an interface device has to authenticate itself against the smart card before the smart card starts any communication. For the authentication of ifd's only short term secrets (passwords) should be used. For this purpose the *icc* should generate a temporary secret for a communication session and has to transfer it in a "secure manner" to the interface device. This requirement ensures that only ifd's which know the current valid shared secret are able to perform a successful authentication. On the other hand attacker cannot start a communication with the contactless smart card without knowing the current valid short term secret
2. an attacker must not learn anything about the valid short term secret if he is able to eavesdrop the communication between *icc* and *ifd*
3. the authentication procedure and the process of key agreement between *ifd* and *icc* to establish a secure channel has to go hand in hand
4. the key agreement procedure has to provide forward secrecy

After a secure and authentic communication relationship between *icc* and *ifd* is established, known smart card security protocols and mechanism can be used to authenticate specific trusted terminals and users. Further discussion on this is beyond the scope of this work.

III Key Establishment and Password-Based Cryptographic Protocols

In the smart card community secret messaging between *ifd* and *icc* is a well-known concept to protect the communication (smart card commands and data) against confidentiality and integrity attacks. Typically a symmetric cryptographic algorithm like the Triple Digital Encryption Standard (3DES) [10] or the Advanced Encryption Standard (AES) is used for this purpose. Furthermore, the data is protected against integrity attacks using Message Authentication Codes (MAC). Instead of using a specific MAC algorithm, symmetric cryptographic algorithms like 3DES can be used for this purpose, too.

But before we can use a cryptographic algorithm for confidentiality and / or integrity protection, strong cryptographic keys have to be established between *ifd* and *icc* for this purpose. Instead of choosing keys by *icc* or *ifd* alone and transfer them to the second entity, a key-agreement algorithm should be used. Hereby both entities are involved in the generation and agreement of a shared key. A well-known protocol which solves this problem very smartly is the Diffie-Hellman key-agreement protocol. Figure 2 demonstrates this protocol in detail.

In the basic Diffie-Hellman key agreement protocol two entities *A* and *B* agree on a generator *g* that generates a multiple group *G* first. Next, *A* and *B* select random values r_A and r_B in the range between 1 and the order of G. A calculates $t_A = g^{rA}$, *B* calculates $t_B = g^{rB}$. Then *A* and *B* exchange the values t_A *and* t_B.. To calculate the shared secret Z_{AB}, *A* calculates $t_B{}^{rA}$ and B calculates $t_A{}^{rB}$. Z_{AB} arises from both calculations. Z_{AB} is called an ephemeral Diffie-Hellman key because it only depends on randomly chosen values.

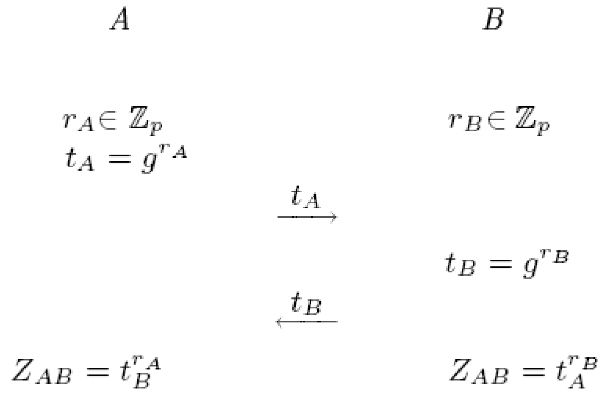

Figure 2 Diffie-Hellman key agreement

The Diffie-Hellman key-agreement protocol has a fundamental limitation. There is no authentication of the messages. Different approaches exist to solve this problem. One interesting approach is to use password-based cryptographic protocols. Password-based protocols have been designed to establish a shared secret between two entities and to built a secure channel and perform an authentication of an entity based on a shared password of small entropy. The idea of Bellovin and Merritt's Encrypted Key Exchange protocol (EKE) [1] is that the protocol initiator chooses an ephemeral public key t_A and uses the shared password π to encrypt this key. The responder chooses an ephemeral public key t_B and encrypts t_B with the password π. In addition the responder chooses a nonce n_B. This nonce is encrypted with a symmetric encryption algorithm using a key K_{AB} which is derived from the ephemeral Diffie-Hellman key Z_{AB}. After the second protocol step the initiator can calculate the ephemeral Diffie-Hellman key Z_{AB}, too. The following protocol steps ensure that only the entities who share Z_{AB} are able to communicate with each other. This protocol steps realize a separate authentication of the initiator and the responder based on the shared ephemeral Diffie-Hellman key Z_{AB}. Figure 3 explains the EKE protocol in detail.

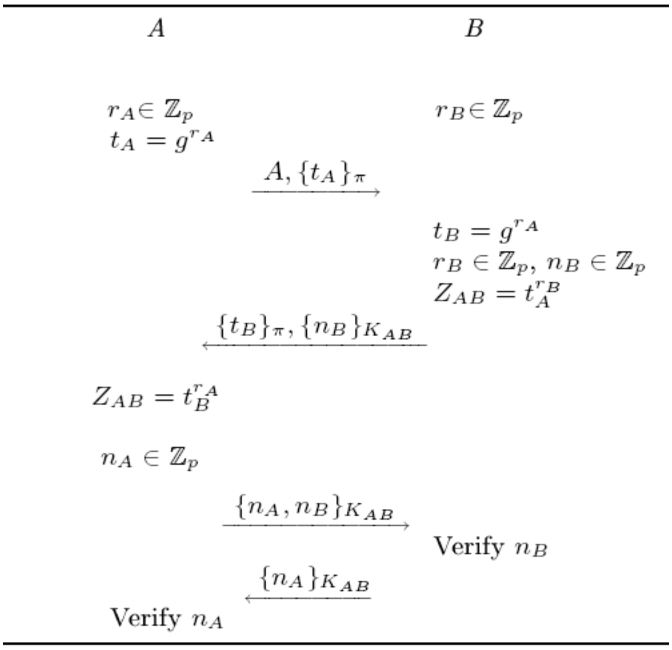

FIGURE 3 ENCRYPTED KEY EXCHANGE

IV THE NEED FOR TWO SEPARATE COMMUNICATION CHANNELS

Now the question arises what we really need to establish secure password (short term secret) authenticated radio frequency channel between an *ifd* and an *icc*? Besides the radio frequency channel an additional channel to transmit a short term secret between *icc* and *ifd* is one possible approach to address the first mentioned security requirement in chapter II. This idea takes into account that only that interface device which knows the current short time secret of the considered *icc* are able to establish a secure radio frequency channel between the considered *icc* and the *ifd*. We might suppose that an optical channel is one technical approach implementing a separate channel. One realization of an optical channel is printing a password on the smart card. But the drawback of this method is obvious. It is sufficient to start an authenticated communication with the *icc* by knowing the printed password. Furthermore it seems theoretically possible for active attackers to store collected passwords in a database. The main disadvantages of this solution are location privacy issues. Static passwords disclose the problem of location tracking. For this reason we suggest using dynamic short term secrets (passwords). Therefore we need an optical device on the card. Our suggestion is to integrate a small visual display unit as a security enforcing component into the smart card. The display is needed to handle the short term secrets (passwords) in combination with password-based protocols as shown in chapter VI. It is important to emphasize that the *iccs* always generates a random short term secret (password) and display them after coming in an electromagnetic field of an interface device. In contrast to the usual deployment of password-based protocols with long term secrets we use random short term secrets (passwords) for the authentication of interface devices and the establishment of password authenticated radio frequency channels.

V FLEXIBLE DISPLAY TECHNOLOGY

Today different flexible display types for the integration in smart cards systems are available. Here we give only a very brief overview of display types:

- Flexible Liquid Crystal Display (LCD) [14]
- Organic Light Emitting Diode Display (OLED)[13]
- Electrophoretic Displays [12]

All display types have different properties. Electrophoretic technology, for example, combine high reflectivity with excellent readability in direct sunlight and very low energy consumption. Further there is no need of a backlight. That is the main energy consumer in most displays. The latter is a very important issue in case of passive contactless smart card systems.

VI SECURE PASSWORD AUTHENTICATED CHANNEL (SPAC)

In our approach we first suggest to use an optical channel for a secure password transmission from *icc* to *ifd*. Secondly, we suppose using a specific variant of a password-based cryptographic procedure. In our approach we combine the basic idea from Bellovin and Merritt [1] with an idea of Boyko et al. [5] using multiplication as a form of symmetric encryption. This is combined with the concept of secure messaging of smart cards. The lather is a well known approach to secure the data transmission between *icc* and *ifd* and vice verse. In general this new approach optimizes the needed protocol steps for establishing a secure password authenticated channel. Figure 4 demonstrates the protocol.

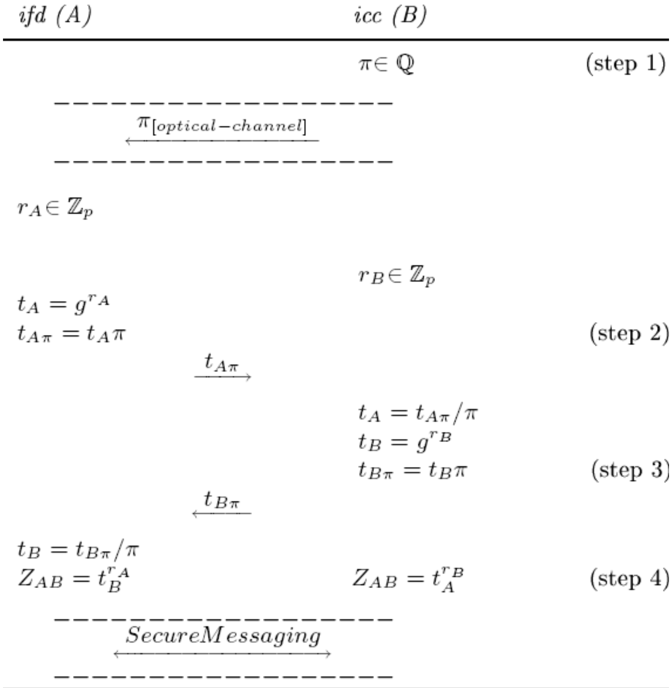

FIGURE 4 SPAC PROTOCOL

First if the *icc* comes into a magnetic field of an *ifd*, the *icc* generates a random short term secret (password) π. In the next step the *icc* displays the password on the visual display unit. The *ifd* then has to read the password. The *ifd* can technically read out the visual display unit with the OCR component scanner or with the help of an user (user keys in the short term secret at the ifd's keypad). Next, the *ifd* generates a nonce r_A to calculate the ephemeral value t_A. In contrast to the classical Diffie-Hellman key agreement, t_A is multiplied by the password π. The *ifd* transmits the result $t_A\,\pi$ via the radio frequency channel. The *icc* calculates t_A with the knowledge of π and figures out the value of the ephemeral Diffie-Hellman key Z_{AB} by choosing a none r_B. Next the *icc* generates the ephemeral value $t_{B\pi}$ as multiplication of t_B and π and transmits $t_{B\pi}$. Now the *ifd* itself can calculate t_B with the knowledge of π. Finally, the *ifd* is able to calculate the ephemeral Diffie-Hellman key, too. But after step 3 of the SPAC protocol the authentication of the *ifd* isn't verified. We suppose to do that implicitly by using the secured data transfer (secure messaging) between *ifd* and *icc* after the SPAC protocol. It is important to emphasize that the data transfer is secured by encryption and message authentication codes. To derive the needed keys K_{ENC} for encryption and K_{MAC} for MAC computation, we recommend following key generation function described in [6, 7]. Both keys are derived from Z_{AB} as described in figure 5.

1. Concatenate $Z_{AB}||c$
2. Use *c=1* for encryption and *c=2* for MAC computation
3. Calculate $H_{ENC}=SHA(Z_{AB}||c=1)$ for encryption
4. Calculate $H_{MAC}=SHA(Z_{AB}||c=2)$ for MAC computation
5. 8 Bytes from H_{ENC} and H_{MAC} respectively form a key

Figure 5 Key Generation

We suggest using secure messaging as specified in [2] chapter 6, Annex E.4. Now an authentication of the entities *icc* and *ifd* can be verified with the first sent data message between *icc* and *ifd* after a successful run of the SPAC protocol. If the verification of the MACs are o.k. then *icc* and *ifd* know that they communicate with the authentic communication partner. If the verification of the first data MAC fails the *icc* has to estimate this as an attack. If so we have to point out that the *icc* has to abort the communication with the *ifd*. Furthermore, we have to protect the *icc* against boundless attacks. Typically, retry counters are used for this purpose. But if retry counters are used in our context attacker can easily enforce denial of service attacks. So in our research, we assesses that wait states are an adequate security solution. We conclude that the icc has to wait *x* cycles after a failed MAC authentication.

VII Brief Security Analysis of SPAC

In the security analysis we distinguish between passive and active attackers. For both cases, we make use of following assumptions. The card owner holds the card. The passive attacker is only able to eavesdrop the radio frequency communication between icc and ifd but not the "optical" communication. This assumption seems realistic for a normal use of the smart card. In this context we have to mention that the readability of the display is only given in a very limited area. On the contrary, the radio frequency communication can be monitored very easily as shown in [8]. An active adversary as opposed to passive attacker can initialize new SPAC protocol runs by guessing passwords. We argue that the potential weakness of the EKE protocol is avoided by using multiplication instead of symmetric encryption.

In figure 4 we suggest to multiply both ephemeral Diffie-Hellman values t_A and t_B with the password π. In order to enhance the performance of the protocol we reconsider the multiplication of t_B in the third protocol step. This seems to have no bearing on the security analysis of SPAC. An active adversary can initialize new SPAC protocol runs by guessing passwords. If we choose passwords with the length of 6 characters and restrict the usable characters e.g. only numerical digits, each password has an entropy of 10^6. If this choice is appraised as insufficient, more characters can be used, e.g. alphanumerical characters. In that case a mapping π -> Z_p is necessary. Here we assume that 6 digits are sufficient. Now an attacker can try to initialize a SPAC protocol run if the card is under control of the card owner (e.g. in the owners trouser pocket). Each attempt to guess a password and to start a new SPAC protocol run enforces the icc to generate a new password π. The probability of an adversary to guess a password can be calculated by the formula shown in figure 6. This formula declares that an attacker has to guess 693146 new passwords to realize a probability of 50 % to guess a right one. In addition, it takes into consideration that each new SPAC protocol run enforces the *icc* to generate a new random short term secret (password) π. With the realistic assumption that one SPAC protocol run lasts nearly 1 second the attacker needs 192,54 hours to enforce the described attack. Moreover, we suppose wait cycles after each failed SPAC protocol runs. As a consequence of our proposal wait states increases the necessary expenditure of time for successfully guessing a short term secret. Fixing the wait state value with respect to denial of service attacks must be in balance between security enforcement and usability consideration. In accordance with this requirement we choose a wait cycle of only one second *(x = 1s)* after each faulty SPAC protocol run. As a consequence, now an attacker requires 2 times 192,54 hours = 385,08 hours for guessing and testing short term secrets.

probability s_n for guessing a password

$$s_n = a + aq + aq^2 + ... + aq^n = a(1 + q + q^2 + ... + q^n)$$

$$s_n = \frac{a(1-q^{n+1})}{1-q}$$

here $a = \frac{1}{1000000}$, $q = \frac{999999}{1000000}$

to achieve a probability of $s_n = 0,5$ $n = 693146$ guessed passwords are needed

Figure 6 Probability Guessing Passwords

Finally we may not forget that an attacker must fulfill a lot of technical requirements before he is able to start a SPAC protocol run. As described in [8] the maximum distance between an adversary *ifd* and an ISO 14443 conform icc may be 25 centimeter at best. In general the range of operation is less then 15 cm.

VIII References

[1] Steven M. Bellovin and Michael Merritt, Augmented encrypted key exchange: Password-based protocol secure against dictionary attacks, Symposium on Research in Security and Privacy, IEEE Computer Society Press, 1992

[2] ISO/IEC 14443, Identification cards - Contactless integrated circuit(s) cards - Part 1 – Part4

[3] David P. Jablon, Strong password-only authenticated key exchange, ACM Computer Communication Review, 1996

[4] Sarvar Patel, Number theoretic attacks on secure password schemes, IEEE Symposium on Security and Privacy, IEEE Computer Society Press, 1997

[5] Victor Boyko, Phillip MacKenzie and Savar Patel, Provably secure password-authenticated key exchange using Diffie-Hellman, Advances in Cryptology - Eurocrypt 2000, Lecture Notes in Computer Science Volume 1807, 2000

[6] Wolfgang Rankl, Wolfgang Effing, Smart Card Handbook, Hauser Verlag, 2004

[7] ICAO, Technical report PKI for machine readable travel documents, version 1.1, October 2004, http://www.icao.org

[8] Thomas Finke und Harald Kelter, Radio Frequency Identification - Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO 14443-Systems, http://www.bis.bund.de/fachthem/rfid/Abh_RFID.pdf, 2004

[9] Ziv Kfir and Avishai Wool, Picking Virtual Pockets using Relay Attacks on Contact-less Smartcard Systems, Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communication Networks, IEEE Computer Society Press, 2005

[10] National Institute of Standards and Technology, Data Encryption Standard (DES), FIPS PUB 46-3, 1999

[11] Ron Rivest, Unconditionally Secure Authentication, Computer and Network Security, Lecture 3: September 11, 1997

[12] Tom Bert, Herbert De Smert, Filip Beunis, Kristiaan Neyts, Complete electrical and optical simulation of electronic paper, Displays journal Vol. 27(2) Elsevier, pp. 50 - 55, 2006

[13] H.E.A. Huitema, G.H. Gelinck, E. van Veenendal, E. Cantatore, F.J. Touwslager, L.R.R. Schrijnemakers, J.B.P.H. van Puitten, T.C.T. Geuns, M.J. Beenhakkers, P.J.G. van Lieshout, R.W. Lafarre, D.M. de Leeuw, B.J.E. van Rens, A Flexible QVGA Display With Organic Transistors, Society for Information Display, 2003

[14] Kang-Hung Liu, Chi-Chang Liao, Yan-Rung Lin, Yu-Chu Hung, Lung-Pin Hsin, A novel flexible liquid crystal display with micro-cell structure, 17th Annual Meeting of the IEEE LEOS 2004, Lasers and Electro-Optics Society