RFID in Bills and Passports

cti.gr

Introduction[1]

Besides the automated tracking capabilities of RFID-tagged goods, RFID tags are also used as an added security feature to thwart counterfeiting, e.g., in high-priced consumer goods such as designer clothing. Plans to incorporate RFID tags into Euro banknotes [1] and passports [2] have repeatedly prompted public concern, due to the sensitive nature of these items. Chips in banknotes are thought to make counterfeiting more difficult, but also help fighting money laundering [3]. In contrast to optical technologies, RFID chips are also thought to be more robust against wear and tear. Similar reasons are given for embedding RFID in passports, along with helping to fight terrorism [2]. Additionally, the contactless read capabilities of RFID chips offer longer lifetimes than the pins of a regular smart card [4].

RFID in Banknotes

Apart from recent confirmations about the type of chip that will be embedded in the Euro banknote (according to a Hitachi spokesperson, the European Central Bank (ECB) is planning to use Hitachi's μ-chip [5]), the only known fact is that the chips are supposed to carry a read-only "38-digit number"[2][5]. This renders mechanisms like hash locks, MetaIDs, or kill-commands useless, as they require writable tags to deactivate or overwrite the original ID[3]. However, giving the (current) owner of a banknote control over the embedded chip would of course contradict the original idea of preventing counterfeiting. Even so, banknotes will probably pose less of a threat to privacy as this might suggest. Even without the help of a blocker tag, the exact number (and denominations) of banknotes an individual carried in her purse would hardly be detectable from a passing thief searching for the next victim. This is because the usage of RFID tags with large read ranges would actually be counterproductive for banks, mer-

chants, and law enforcement agencies alike, as this would make it difficult to relate a digital ID that has been read with the specific banknote in hand. Not surprisingly, the chosen μ-chip has a read range of just one millimeter [9]. Even if tags with a slightly higher range were used, and thieves would use crowded subway-trains to approach their victims, a purse lined with aluminum foil would easily spoil such attempts. Even without such a protection, having several banknotes aligned and stacked would significantly detune each of the tags, thus thwarting any read attempt of the entire stack[4].

Another often-cited attack against RFID-enabled banknotes would be an increased, if not comprehensive, tracking of each individual banknote, including correlating each banknote to the person receiving or spending it. Merchants already have much easier tools at their disposal to learn individual shopping behavior, e.g., in the form of the increasingly ubiquitous loyalty cards. This is not only much cheaper than installing costly new banknote scanners, but also (and more importantly) legal, as consumers give their consent to such data collections upon signing the loyalty card application form. In order to execute such a scheme on a national, if not global scale, a central merchant-register for currency tracking would need to be installed – the number of parties involved in such a process makes this both economically and politically unlikely. The example given by Juels and Pappu [7] of several merchants secretly sharing their banknote data would not only be a severe violation of existing laws in many countries, but could again be implemented in a much cheaper and politically safer manner through a multi-merchant loyalty card, much like the card issued by the Payback group in Germany[5]. Similarly, fears of tracking banknotes through a writable "memory" chip that would "allow money to carry its own history by recording information about where it has been, thus giving governments and law enforcement agencies a means to literally 'follow the money' in every transaction" [10] seem unfounded, given the significant necessary investments in national and international monetary infrastructure to implement this, and of course the current chip's lack of writable memory. RFID chips are thus only useful as another technical hurdle for reproducing counterfeit banknotes. Given the chosen, proprietary RFID technology from Hitachi, counterfeiters would need access to chip fabs capable of

producing µ-chips with their 0.18 micron structures [6]. However, in order to detect a fake RFID chip (should counterfeiters ever be able to reproduce them)[6], or for following a "hot trail" of blacklisted money from a robbery or kidnapping, a central database run by the ECB might still be necessary, in which national and private banks, as well as merchants, might perform verification lookups. Such a central certification register would then be able to detect not only blacklisted IDs, but also identify duplicate banknotes if the same ID is submitted from two or more geographical places in too short a time that would allow for a single banknote to travel between these two places. Similarly, IDs that would be checked (on average) more often than others might also imply a duplicated banknote [11]. However, RFID tags in banknotes will probably not help the average citizen to better identify counterfeit money, as such chips would be embedded invisibly and thus only detectable with corresponding readers[7].

Work on technical privacy-protection tools for RFID-tags has therefore focused on reducing the amount of detail reported by such tags, e.g., by replacing the stored serial number with a generic manufacturer code or even a completely arbitrary number, and on preventing any unnoticed read-outs of such tags. Due to the envisioned widespread usage of such tags, the former method might only be a partial solution: Even if the level of detail provided by such tags is significantly reduced, the specific combination of tags carried by an individual, socalled "constellations" [1], might still allow for the identification of a person. Existing technical solutions in the field of RFID privacy can be divided into anonymizing and pseudonymizing methods. Both can either be achieved by deleting or altering the data on the tag itself, or by controlling read access to it. Especially the latter is critical, since RFID readers must also provide the energy to power the battery-less tags, resulting in reader-to-tag communication that stretches much further than the corresponding return channel from the tag back to the reader.

RFID in Passports

In contrast to RFID in banknotes, embedding RFID chips in passports is already a reality. After the International Civil Aviation Organization (ICAO) approved the latest specification for "machine readable travel

documents" (MRTD) in May 2004[8], the US State Department began issuing RFID-enabled passports to diplomats and State Department employees from January 2005 [13]. On December 13, the European Union's Council of Ministers similarly decided to mandate that within 18 months, all passports issued in EU member countries must carry not only the MRTD-mandatory biometric facial image information, but also a digital representation of the holder's fingerprint[9][14].

The EU plans also include another optional feature from the MRTD specification, namely an optical access control similar to the one proposed by Juels and Pappu [7] for banknotes: the access key for the RFID chip is computed from the already available machine-readable (through optical character recognition) data on the passport, the socalled "machine readable zone" (MRZ) [4]. Readers must first optically read the passport number, birthdate of the holder, and expiration date of the passport. After computing a hash value from this information, a reader contacts the RFID chip embedded in the passport to receive a random number, which it encrypts using the computed hash value. The reader also chooses a random number of its own, as well as one half of the session-key that should be used for the actual data transmission. Encrypting all three parts with the computed hash value, the readers sends this back to the RFID chip, which in turn verifies that its own random number was correctly encrypted, after which it then decrypts the reader-chosen random number and the session-key part. The final step is then for the RFID chip to encrypt the reader-chosen random-number again using the hash-value, as well as a session-key part of its own, and send both back to the reader. The result is that both reader and RFID chip now have a complete session key (each half chosen by one of the two), upon which the actual data transmission can begin [4]. While the complexity of the hash-value used for decrypting this initial key exchange is high enough[10] to prevent an eavesdropping attacker from learning the chosen session key values and subsequently decrypting the actual biometric information, a recording of this communication could be attacked with more time and increased computing resources, in order to first deduce the initial hash value, and with this the session keys used for the actual data transfer [4].

Another complication arises from RFID-enabled visas, which, according to EU plans, should use similar mechanisms to increase their authenticity [15]. However, just as several stacked RFID-enabled banknotes will detune the individual tags so that reading all tags becomes almost impossible, the combination of an RFID-enabled passport with one or more RFID-enabled visa stickers will make the automatic reading process highly unreliable [16].

In contrast to RFID chips on milk cartons or clothing tags, the application of contactless identification technology in passports could have significant security implications. While the use of an optical key will most likely prevent "that pickpockets, kidnappers and terrorists can easily – and surreptitiously – pick Americans or nationals of other participating countries out of a crowd" [17], a determined attacker might still learn the data required to compute the optical key (passport number, birthdate, passport expiration date) for a particular individual and, using a sufficiently powerful reader, quickly scan a group of people[11].

Marc Langheinrich received a master's degree in computer science from the University of Bielefeld, Germany, in 1997. He spent a year as a Fulbright Scholar at the University of Washington in Seattle, USA, and two years as a researcher at NEC Research in Tokyo, Japan. Since October 1999 he is a research assistant in the Institute for Pervasive Computing at the ETH Zurich, Switzerland, where he investigates the intersection of privacy and ubiquitous computing, both from a technical and social perspective. Marc is one of the authors of P3P, an emerging standard for exchanging privacy policies on the Web.

[1] This work is based on an earlier article (in German) by the same author: Marc Langheinrich „Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie." In: Elgar Fleisch, Friedemann Mattern (Eds.): *Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis*, Springer-Verlag, 2005.

[2] It is not yet clear what is actually stored on these tags. While 38 digits would be enough to store the 10-digit serial number, the (sin-

gle-letter) country code of the issuing bank, the 6-digit “short code” (the short code identifies the printing origin, see www.myeuro.info/euro-snr. php), and any required checksum information, the complexity of synchronizing the printing process with the fab-initialized µ-chips might prompt the ECB to instead keep a database associating random chip serial numbers with banknote serial numbers after production [6].

[3] Notwithstanding, Jules and Pappur [7] earlier proposed a system using a combined optical and radio-based approach, which also requires writable RFID tags. The optical data consists of a printed access key, which is required in order to read and optionally write the information stored on the RFID chip. Without the key, only an encrypted serial number of the banknote can be read. Merchants are supposed to re-encrypt the serial number with a random number whenever they receive a banknote, in order to prevent tracking attacks. The random value is stored in the key-protected area of the banknote as well, thus allowing anybody with optical contact to the banknote to first decrypt the random value, and then decrypt the serial number (and, ultimately, to choose a new random value, re-encrypt the serial number, and store this new random value again). Avoine [8] has shown that the proposed mechanism does not actually require optical access to the banknote in order to successfully decrypt the serial number, and that attackers can still track such banknotes.

[4] This effect would also prevent any automated inventory taking of a whole stack of money in a bank, similar to the envisioned supply-chain stock-taking of RFID-tagged products, that some magazines alluded to [12].

[5] Payback loyalty cards are accepted at more than a dozen national retailers throughout Germany. See www.payback.de.

[6] Once counterfeiters are able to incorporate an RFID chip with the right dimensions into a banknote, having it respond with the same (static) ID as a valid banknote is trivial to achieve, even if this ID has been cryptographically signed.

[7] Though future mobile phones might include RFID readers capable of reading µ-chips and doing a lookup in realtime.

[8]

[9] The MRTD specification requires that each passport carries a digital representation of the holder's facial image, and a digital signature from the issuing country. Countries can optionally also include fingerprints and iris scans [4].

[10] Kügler [4] compares the complexity of the MRZ-based information to a 56-bit key such as DES.

[11] Again, using a face recognition system capable of identifying individuals in spite of superficial changes in appearance (such as mustaches or hair color) might be more reliable, as it also does not require the target to carry his or her passport with her.