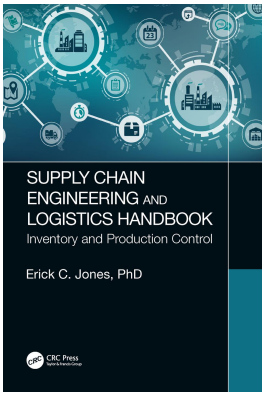

Supply Chain Engineering and Logistics Handbook Inventory and Production Control

Erick C. Jones

Secure Documents with RFID and Potential Blockchain Implications

Publication details
https://test.routledgehandbooks.com/doi/10.1201/9781315159096-18
Erick C. Jones
Published online on: 05 Dec 2019

18

Secure Documents with RFID and Potential Blockchain Implications

Erick C. Jones

The EOQ model at it's core can validate or invalidate Quality management theories.

Erick C. Jones

18.1 Secure Document RFID Applications

18.1.1 Introduction

Perhaps the most sensitive radio frequency identification (RFID) application to date involves the use of RFID technology with government passports. The issuance of the U.S. Electronic E-Passport began on August 14, 2006. E-Passports contain the same information as conventional passports but also include an RFID chip in the rear cover of the passport. Since the first E-Passports were issued, a great deal of public criticism has arisen. Some tests by independent parties indicate that it is possible to overcome the built in security and privacy measures incorporated into E-Passports. However, whether or not these potential weaknesses can be illegally exploited by illegal aliens and terrorist groups has yet to be determined. In this chapter, we will begin with a basic description of how the E-Passport functions and continue with a discussion of security issues.

18.1.2 Basic Passport Background

Passports are issued by virtually all nations. They are usually required for identification purposes for entry into most nations. The few exceptions to this requirement that do exist are slowly being eliminated. For example, the Intelligence Reform and Terrorism Prevention Act of 2004 required the U.S. Department of Homeland Security and the U.S. State Department to develop and implement a plan whereby all travelers need a document such as a passport for identification purposes on entry into the United States. As a result of the act, since January 23, 2007, all persons, including U.S. citizens traveling by air are required to have a passport or similar documentation for entry from Mexico and the Caribbean. As early as January 1, 2008, these requirements may be extended to both land and sea.

The passport currently being issued by the Department of State is the E-Passport.

Note that the page contains a photograph, the passport number, the individual's name, date of birth, birth place, sex, and passport issue and expiration dates. The E-Passport also contains an RFID chip on the inside back cover of the passport. The inside back cover is illustrated in the following Figure 18.1.

Since the passport issuing period is 10 years, it will be a number of years before all of the passports in circulation will be required to be renewed. Until then, it is anticipated that all of the non-E-Passports in circulation will continue to be valid.

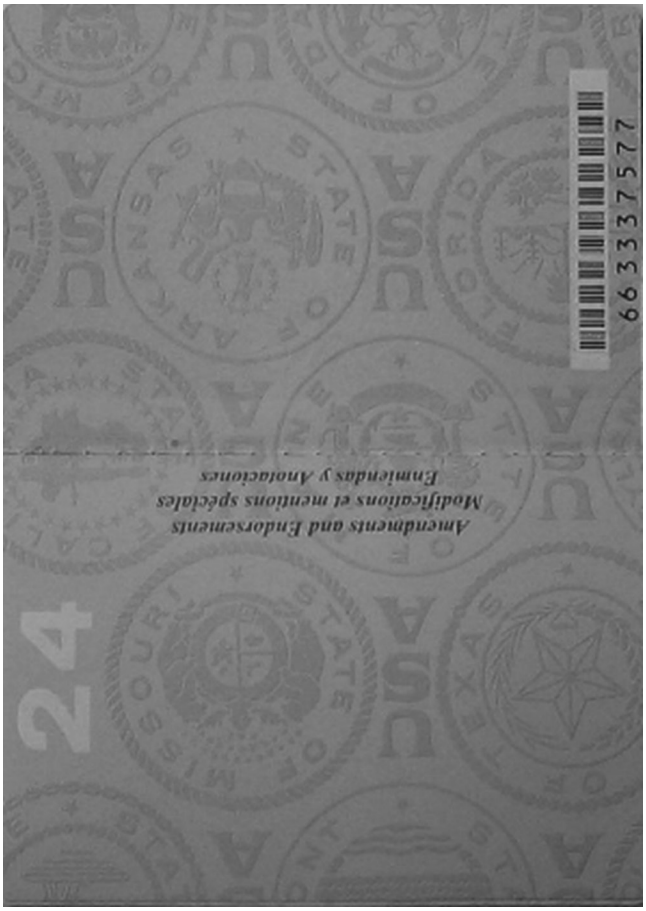

FIGURE 18.1 Inside back cover of E-Passport.

18.1.3 E-Passport RFID Chip

The E-Passport RFID chip contains 64K of encrypted data. Publicly accessible sources indicate that the chip holds the same information that is available on the picture page of the E-Passport. As we stated earlier, this includes the passport number, the individual's name, date of birth, birth place, sex, and passport issue and expiration dates. The chip also includes a digital photograph of the passport holder. The presence of the digital photograph allows for the possibility of incorporating biometric identification systems at some future point in time. This means that an individual may be digitally scanned at the point of entry. The real-time scan would then be biometrically compared to the digital photo contained in the RFID chip. The exact contents of the chip are governed by the International Civil Aviation Organization (ICAO), which we will discuss in the next section.

18.1.4 ICAO Protocol

The E-Passport follows the standards indicated by the ICAO. These standards are available from their website at www.icao.int/mrtd/download/technical.cfm [1]. One of the significant components of this protocol is that the E-Passport is only supposed to be readable from very short distances. This is officially reported as 4 in. However, there are some claims that E-Passports can be read as far as a few feet away. The unauthorized reading of passports by unknown individuals has been termed as "skimming".

To combat successful skimming, the U.S. State Department has incorporated a multi-layered security system to help prevent the unauthorized access of E-Passport data. The first layer of protection consists of electronic shielding built into the cover of the E-Passport. This is intended to block signals from any RFID readers attempting to energize the E-Passport and read the resulting signal [5].

The second level of security is what is known as Basic Access Control. This begins with a sequence of machine-readable characters physically printed on the E-Passport. This sequence of numbers is an encryption key. When the passport control officer scans the E-Passport, the RFID reader uses the encryption key to communicate and decode the data from the RFID chip [4]. In theory, this means that the only way to obtain and decode the data on the E-Passport is to first open up the passport and obtain the encryption key.

Critics of the Basic Access Control system are not so optimistic. In the summer of 2006, German hackers succeeded in successfully accessing ICAO-based passport data. By reading the publicly available ICAO documents, the hacker determined that the encryption key was based on information contained on the passport photo page [2]. The hacker was then able to crack an electronic passport and download the information to a smart memory card. By inserting the smart card into a physical passport, the hacker was able to present different physical and RFID passports.

An additional security measure used with E-Passports is known as a Public Key Infrastructure (PKI). The mechanics behind the PKI are beyond the scope of this chapter. However, it should be understood that the purpose of the PKI is to help insure that the data in the E-Passport RFID chip cannot be altered. It is in essence, a digital signature. In the event that the data is altered, the digital signature created with the PKI will indicate that tampering has occurred. For the individual, this also means that any change in name or other data will require that an entirely new passport be obtained. To help minimize the potential burden to citizens, the U.S. Department of State is allowing new passports to be obtained without charge for 1 year.

Another security problem associated with E-Passports is known as "eavesdropping". This is the electronic monitoring of the signals between the RFID reader and the E-Passport. The possibility of this has also been demonstrated as a group of Dutch hackers successfully eavesdropped on an RFID transmission and within 2 h successfully decrypted a digitized fingerprint, photograph, and other text information from an E-Passport in February of 2006 [3]. Since the Dutch E-Passport is based on the ICAO standards, it is presumed that this may also be performed on other ICAO standards-based E-Passports. The current government response to this potential weakness is to maintain electronic eavesdropping detection equipment at ports of entry.

18.1.5 Other Developments

Late in 2006, the Department of State announced the possibility of augmenting E-Passports with a Passport Card. The passport card is intended to simplify travel between the United States, Mexico, Canada, and the Caribbean. Like the E-Passport, the Passport Card will incorporate an RFID chip. However, at this time, the Passport Card is not expected to incorporate personal information in the same manner as the E-Passport. Instead, the Passport Card will be linked to a central database which contains the individual's photograph and biographical data. The Passport Card will also be more convenient and significantly cheaper to acquire than an E-Passport.

18.1.6 Deployment

It will likely be some time in the future before E-Passports outnumber the number of conventional passports in circulation. In addition to replacing the conventional passports with E-Passports, the Port of Entry facilities must also have the optical scanners and RFID readers that the E-Passport RFID chips need to operate. As this equipment is installed, the access lanes will be marked with the special international E-Passport symbol illustrated in Figure 18.2. This will allow travelers to properly take advantage of the increased capabilities of their E-Passports. It is expected that this will help speed the processing of travelers.

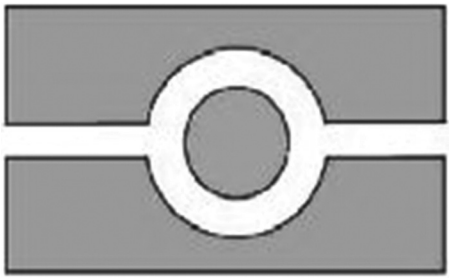

FIGURE 18.2 E-Passport lane symbol.

18.1.7 Summary

The use of E-Passports offers potentially faster processing of individuals through port of entry facilities. Faster processing is possible as the same information that is available on the picture page of the passport is also stored in the RFID chip. When the passport is optically scanned, the RFID chip transmits this information to the control point. The immigration agent can then check the passport record against immigration records and watch lists.

The technology inherent in RFID chips have led to a number of concerns with respect to the data security of E-Passports based on the ICAO standards. Independent tests have indicated that RFID E-Passport data can be both cloned as well as eavesdropped on by unauthorized parties. However, the issuance of E-Passports is still proceeding. Proponents of the use of E-Passports dismiss these security concerns, stating that the use of RFID technology is intended as an additional security measure rather than a replacement to the function of a conventional non-RFID passport.

REFERENCES

[1] International Civil Aviation Organization Protocol. www.icao.int/mrtd/download/technical.cfm
[2] Miller, P. German Hackers Clone RFID Passports. www.engadget.com/2006/08/03/german-hackers-clone-rfid-e-passports/
[3] Ricker, T. Dutch RFID E-Passport Cracked—U.S. Next. www.engadget.com/2006/02/03/dutch-rfid-e-passport-cracked-us-next/
[4] Schneider, B. RFID Passport Security Revisited. www.schneier.com/blog/archives/2005/08/rfid_passport_s_1.html
[5] Department of State Begins Issuing Electronic Passports to the Public. https://2001-2009.state.gov/r/pa/prs/ps/2006/70433.htm