Security of Horse Animal Identification & Registration in The Netherlands

Laurens Bruinsma
Vic Ding

February 2010

UNIVERSITEIT VAN AMSTERDAM

Security of Horse Animal Identification & Registration in The Netherlands

Research report for System and Network Engineering, MSc education at the University of Amsterdam, The Netherlands.
Conducted under supervision of Jeroen van Beek from Dexlab.

Security of Horse Animal Identification & Registration in The Netherlands

Abstract

EU and national legislation dictate that all domestic horse animals aged 7 months or older should have a passport document and an implanted RFID tag that identify them. Both contain a transponder number that is used to verify the identity of an animal.

Goals of the system of identification and registration are:

- Preventing / discouraging fraud in sports and trade
- Preventing / discouraging theft
- Protecting food safety by recording administering of medicine
- Facilitating administration of medical treatment by veterinarians

In this research, the security of the system is evaluated. This is done by defining performing a risk analysis based on the CIA model for information security.

Results of the research are that cloning of a tag is very feasible because of the absence of authentication checking.
Furthermore, forging of passport documents is also feasible, as it has very few security features.
Finally, data processing and storage is mostly performed locally at the location of the 31 passport issuing organizations. As a result, many people have (write) access to this data, which poses a security risk.

We recommend to implement an authenticity checking mechanism into the RFID tags and readers to prevent cloning. If this is not possible, we recommend to implement online checking possibilities (e.g. a website) to be able to easily look up full information about a certain animal.
Furthermore, we recommend defining a set of adequate security features that make it more difficult to successfully forge a document and that make it easier to detect forgeries. We recommend to implement these security features in all new documents.
Finally, we recommend considering setting up a central organization to carry out the process of identification and registration of horse animals, instead of the current decentralized system consisting of a central organization plus 31 passport issuing organizations.

Acknowledgments

We would like to thank the following persons and organizations for their help during our research project:

Jeroen van Beek, Dexlab

Stal Zadelpret , Waverveen

Product Board for Meat and Livestock

Virbac Nederland B.V.

Merens Stud-book

Arabische Volbloedpaarden Stud-book

KFPS Stud-book

Welsh Pony & Cob Stud-book

Paardenkliniek Garijp

WPCV Stud-book

Table of contents

1 Introduction

1.1 Background

In the Netherlands, all domestic horse animals aged 6 months or older should have a passport document that identifies them. It is also mandatory to implant an RFID tag in the neck of the animal. These rules are based on European legislation[1], on which a national regulation[2] is based. The tag has a transponder number that is also printed in the passport document. By comparing these two numbers, one can verify the identity of the animal (provided that both numbers are authentic). Besides the transponder number, every animal has a unique identification number that does not change during it's lifetime. This number is also printed in the passport document.

Goals of identification are:

Protecting food safety

This is the main goal and is the reason why the system was introduced.
When an animal is not intended to be slaughtered for human consumption, this is registered in the passport document. In this case, a more relaxed policy for administering medicines applies. If nothing is registered in the passport document, then it is assumed that the animal is intended for human consumption and strict medicine policy automatically applies.

Preventing / discouraging fraud in sports and trade

Horses, especially those used in races, can be very expensive. Therefore, fraud can be very lucrative. The possibility to verify the identity of an animal should help to prevent fraud.

Preventing / discouraging theft

Because all animals should have a passport document, a potential buyer can ask for this and check it. Furthermore, the buyer could verify if the transponder number that is printed in the passport document corresponds to the read out of the RFID tag that is implanted in the animal.

Administration of medical treatment

A veterinarian could use the transponder number or the identification number of an animal for his or her administration of medical treatment of the animal.

Because the described stakes are considerable, it is key that the security of the system is adequate. Insecurity may even open up scenarios that would not have been possible in a system without RFID tags and passport documents.

1.2 Overview of the system

The system of identification and registration of horse animals is dictated by European legislation, as already mentioned in paragraph 1.1. Each EU member state has to implement this legislation nationally. In The Netherlands, this is done by the means of regulations from PVV, the Product Board of Meat and Livestock. However, most of the system itself is implemented by a number (currently 31) of 'passport issuing organizations' that are authorized by PVV. They have to adhere to the regulations of PVV. Most of the organizations are stud-book organizations. The KNHS, a general horse sports organization, is also authorized to issue passport documents.

1.2.1 RFID tags and readers

The RFID tag consists of a very small integrated circuit and antenna, which are encased in bio-glass or a bio-polymer. The size of the tag is comparable to that of a grain of rice.
The tags and readers used in the system must comply to ISO standards 11784 and 11785. The former standard describes the structure of the transponder number that is on the chip. The latter standard addresses how the RFID reader communicates with the RFID tag.

The meaning of the digits of a transponder number is specified in table 1.

Country code (ISO 3166-1)	3 digits NL: 528
National code	12 digits, governed by each nation NL: 4th digit: 1 for user group, 2 for manufacturer 5th, 6th (7nd) digit: specification of user group or manufacturer 7th (8th)-15th digit: unique number determined by manufacturer

Table 1: Transponder code structure

The 'Country code' need not necessarily denote a country: codes 900 to 998 may be used by manufacturers, who can acquire a code from the ICAR organization. Code 999 is used for testing purposes.
The structure of the 'National code' part of the number is decided by every

country independently. For this reason, it differs greatly per country or even within a country itself (Germany)[3].

The Dutch authorities only recognize RFID tag manufacturers that produce tags that comply with ISO 11784 and 11785 standards[4]. Additionally, only the Dutch country code '528' may be used, and the manufacturer has to submit information on manufactured tags to a special agency of the Ministry of Agriculture (Dutch: 'Dienst Regelingen') that ensures uniqueness of manufactured transponder numbers.
Besides the officially approved tags, there are many other brands of tags for sale, especially on the internet. One manufacturer indicated that they program additional, secret data onto the chip, to be able to distinguish it from imitation chips[4].

In figures 1, an actual RFID tag of the type that is used with horse animals is displayed. In figure 2, the needle that is used to implant the tag is displayed. Figure 3 is a picture of a professional RFID reader. The length of the tag is about 12 mm.

Figure 1: RFID glass tag

Figure 2: Insertion needle

Figure 3: Professional RFID reader

1.2.2 Passport documents

As their name suggests, the passport issuing organizations mentioned in section 1.2 issue the passport documents.

The EU legislation[1] states which information should be stored in the document:

A. The passport must contain the following information:

1. Sections I and II — Identification (including transponder number)

2. Section III — Owner

3. Section IV — Recording of identity checks

4. Sections V and VI — Vaccination record

5. Section VII — Laboratory health tests

6. Section VIII — Validity of document for movement purposes

7. Section IX — Administration of veterinary medicinal products

Source: EU regulation 504/2008

Security of Horse Animal Identification & Registration in The Netherlands

Security related document document features are not dictated by legislation.

In figures 4 and 5, some pictures of passport documents are shown.

Figure 4: Horse passport cover

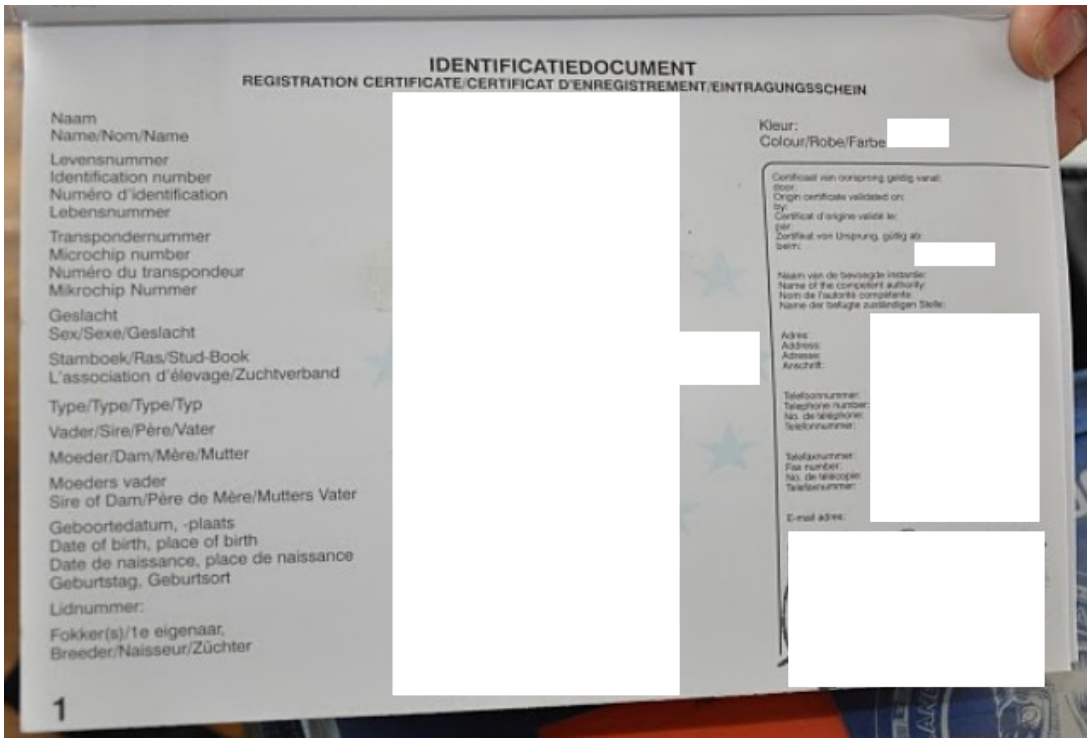

Figure 5: First page of horse passport

1.2.3 Registration process

The registration of animals is carried out by the passport issuing organizations mentioned in section 1.2. They process and store information about the animals' identities.
Besides this decentralized administration, there is also a central database administrated by PVV[5]. This database contains all transponder number that are issued by the passport issuing organizations and their associated animal identification numbers. It provides a means to check whether a certain transponder number is already in use and if so, which organization issued the transponder number.
The passport issuing organizations have to store detailed data about an animal at least 35 years for a living animal. When an animal dies, data have to be stored for at least another 2 years.

1.3 Research focus

In this project, the security of the system of (electronic) identification and registration of horse animals is be evaluated. The following topics are covered:

1. Security of RFID tags and readers
2. Security of passport documents

3. Security of data processing and storage
4. Security of procedures

The emphasis of this research is on security of RFID tags and readers and the security of procedures. Researching the data processing and storage back ends on location of the passport issuing organizations and PVV is outside the scope of this research.

We have formulated the following research questions:

1. *What general security requirements should the system meet?*
2. *What risks is the system imposed to?*
3. *How can the security of the system be improved?*

1.4 Research methodology

I) Defining high level security requirements for the system that are based on the CIA model.

II) Performing a risk analysis, looking at these aspects of the system:
- RFID tags and readers
- Passports documents
- Data processing and storage
- Procedures

III) Formulating controls that mitigate the identified threats.

IV) Investigating the current situation and determine to what extent defined controls are actually implemented.

V) If risks/weaknesses are identified in step IV: formulating recommendations.

1.5 Structure of the report

In chapter 1, this introduction, we introduce the research topic by providing background information about the system of horse animal identification and registration. Furthermore, research questions are formulated, some insight into the used research methodology is given and related work is mentioned.
In chapter 2, high level security requirements based on the CIA model are formulated.
Chapter 3 contains the results of the risk analysis of the system.
Controls to mitigate the identified risks are defined in chapter 4. In that chapter,

also the findings of the analysis of the current situation are documented, accompanied by recommendations when applicable.
Finally, conclusions are drawn in chapter 5. Furthermore, the research results are discussed and suggestions for future research are done in that chapter.

Appendix A contains logs from RFIDIOt, a tool for writing to and reading from RFID chips.

2 Theoretical background: CIA model

The CIA model is widely accepted as a basis for information security[17][18][19]. It is used in this research to define high level security requirements for the system of horse animal identification and registration. These requirements will be used as a basis for the risk analysis that is performed in chapter 3.

2.1 Confidentiality

Confidentiality prevents the disclosure of information contained in the chip or during the data processing to be read/written in anyway by any unauthorized person or by an authorized person at improper time and/or with malicious intention.

Since the chip is for tagging purpose, it is not secured at all. The only information stored on the chip is the hex-encoded value of the ISO-11784 horse ID. There will be no disclosure of confidential information even if it is read by any party.

However, during the data processing time, if there is information leakage of sensitive data like birth, death etc, then the confidentiality cannot be ensured. Especially data about the owner of a horse should be regarded as confidential. The same holds also true for passport documents.

2.2 Integrity

Integrity means that data should not be able to be modified without authentication and authorization. It consists of four parts, as listed below:

-Data integrity: This is the basic of all the other parts. It is the “correctness” of data. Data itself should not be changed by accident or by any unauthorized person. In our case, for the chip the data integrity is quite ensured as the chip is read-only, though the database of the registration unit can be vulnerable.

-Accountability: Accountability is that after a record status change was made in the database, it is not able for any party to deny the fact that they've made commitment or any party was impersonated that was involved in the procedure.

-Authenticity: Authenticity ensures that only the desired person with the proper privilege can do the desired action to the system. In our case, the database system at registration unit should only be operated by authenticated personnel.

-Authorization: Authorization means that only persons with proper permission can carry out a certain operation on the designated database.

2.3 Availability

Information should be available whenever it is needed. Availability is the healthiness and strength of the information and the system in which the information is contained. Availability can be impaled in many ways, i.e. by jamming the communication channel between the chip and reader, a DoS attack and physical damage to the system.

3 Risk analysis

In this section, risks regarding the system of horse animal identification and registration are identified. The CIA triad is used as a basis for this: risks are classified according to this model.
The following four components of the system are taken into account in this analysis:

1.RFID tags and readers
2.Passport documents
3.Data processing and storage
4.Procedures

The risks that are covered in this chapter are *potential* risks: it may turn out that some of them are, in practice, not very significant. For example, it may be the case that certain attacks are possible, but that there are other attacks that are much easier to carry out. When this is the case, it will be noted in chapter 4.

Note: When no risks of a certain type are identified for a certain part of the system, this is noted by *None.* Furthermore, when a certain type of risk is not applicable to a system component, this is noted with *Not applicable.*

3.1 Confidentiality

- ***Risk scenario: Confidential information, i.e. about animal owners, gets disclosed.***

RFID tags and readers	
Risk:	None

The only information available on the RFID tag is the hexadecimal value of the transponder number. The release of this number will not create a revealing of confidential information. So the confidentiality is not our concern, but it does open other chance for other kind of attacks. These risks are covered in paragraph 3.2.3 (Authenticity).

Passport documents	
Risk:	None

A passport document contains some confidential information, i.e. information

regarding the owner, but by nature, the document will not be widely accessible like the data in a database may be (see below). Therefore no risks are formulated.

Data processing and storage	
Risk:	Attackers might gain unauthorized access to the database by abusing software bugs, configurations issues and easy to guess passwords.

Procedures	
Risk:	Not applicable

3.2 Integrity

3.2.1 Data integrity

- ***Risk scenarios: not applicable. Data integrity is relevant for the risk scenarios defined in the other sections of the risk analysis.***

RFID tags and readers	
Risk:	There is no protection against unauthorized tampering with data on the chip.

Passport documents	
Risk:	The passport document does not have adequate security features.

Data processing and storage	
Risk:	No adequate measures in place to ensure data integrity of a database.

Procedures	
Risk:	Not applicable

3.2.2 Accountability

Risk scenarios:

- ***Nobody can be held responsible for the security of the system.***
- ***Animal ownership cannot be determined.***
- ***Changes to the registration of animals cannot be traced.***

RFID tags and readers	
Risk:	Responsibility ('business owner') for security of RFID tags and reader is not (well) defined.

Passport documents	
Risk:	Responsibility ('business owner') for the security of passport documents is not (well) defined.
Risk:	Issuing and revoking of passport documents cannot be traced.

Data processing and storage	
Risk:	Responsibility ('business owner') for the security of data processing and storage is not (well) defined.
Risk:	Changes to the contents of a database cannot be traced.

Procedures	
Risk:	Responsibility ('business owner') for the security of procedures is not (well) defined.
Risk:	Deniable transaction: After the transfer of ownership, one party is able to deny the fact that he has made commitment, and hence want to reverse the process to re-obtain the ownership or not to admit that he was the previous/current owner of the horse.

3.2.3 Authenticity

- ***Risk scenario: Animal identity is unauthentic***

RFID tags and readers	
Risk:	Impersonating a genuine tag by: copying/cloning plain read crypto attack side channel attack eavesdropping on the communication between tag and reader
Risk:	There is more than one tag with the same transponder number in the system.

Passport documents	
Risk:	Spoofing the identity of an animal with an existing, genuine passport document.
Risk:	Obtaining a blank passport and creating a false identity with it.
Risk:	Altering a genuine passport to change the identity (i.e. breed) of the associated animal.

Data processing and storage	
Risk:	Because researching risks regarding this matter is outside the scope of the research, no risks have been defined.

Procedures	
Risk:	An animal that is not intended for human consumption gets in the food chain (for humans).

3.2.4 Authorization

- ***Risk scenario: Unauthorized adding, changing or removing of animal identities.***

RFID tags and readers	
Risk:	Unauthorized changing of the contents of the chip: -chip is writable -chip appears to be not writable (emulation), but in fact is

Passport documents	
Risk:	Unauthorized modifying of the passport.

Data processing and storage	
Risk:	An unauthorized person changes contents of a database.

Procedures	
Risk:	Unauthorized first registration of an animal.
Risk:	Unauthorized unregistering of an animal (e.g. when an animal dies.
Risk:	Unauthorized reregistering (i.e. when a new passport or RFID chip is issued) of an animal.

3.3 Availability

- ***Risk scenario: Identification and/or registration of animal identities is (temporarily) not possible.***

RFID tags and readers	
Risk:	Tag gets permanently disabled by: –tag removal –tag destruction –KILL command (a special command implemented in certain RFID chips) –normal 'wear and tear'
Risk:	Tag gets temporarily disabled by: –passive interference

	–active jamming –relay attack

Passport document(s)	
Risk:	The passport gets damaged due to poor material quality.
Risk:	The passport gets lost due to: - theft - accidental loss

Data processing and storage	
Risk:	The information in the database becomes unavailable, i.e. due to: - dos attack on the database server - hardware failure - a disaster, like a fire - accidental removal of some or all information (i.e. by a junior system administrator) - network failure

Procedures	
Risk:	Not applicable

4 Controls, findings and recommendations

In this chapter, controls are formulated that can mitigate the risks that are formulated in chapter 3. Furthermore, the findings of the current situation regarding each control are described: To what extent is the described control already implemented? When applicable, recommendations are made.

4.1 Confidentiality

- ***Risk scenario: Confidential information, i.e. about animal owners, gets disclosed.***

RFID tags and readers	
Risk:	None
Control:	Not applicable
Finding:	**F1**: The only information available on the RFID tag is the hexadecimal value of the transponder number. The release of this number will not create a revealing of confidential information. However, it does open up possibilities for other kind of attacks. These risks are covered in section 4.2.3 (Authenticity).
Recommendation:	Not applicable

Passport documents	
Risk:	None
Control:	Not applicable
Finding:	**F2**: A passport document contains some confidential information, i.e. information regarding the owner, but by nature, the document will not be widely accessible like the data in a database may be (see below). Therefore no risks are formulated.
Recommendation:	Not applicable

Data processing and storage	
Risk:	Attackers might gain unauthorized access to the database by abusing software bugs, configurations issues and easy to guess passwords.

Control:	The database should only be accessible via the front end user interface and should not be writable by unauthorized persons.
Finding:	**F3**: There is only one organization[6] that has an online check function of their database content. This function is very limited. We could not further test the security of the site because that would have been illegal. We found that the MySQL database is accessible from the Internet by port 3306. It is not an issue if the database is properly secured. However, if there is no explicit usage of the port, it is always more secure to close the open port.
Recommendation:	Close port 3306 on the server for Internet users.

Procedures	
Risk:	Not applicable
Control:	Not applicable
Finding:	Not applicable
Recommendation:	Not applicable

4.2 Integrity

4.2.1 Data integrity

- ***Data integrity is relevant for the risk scenarios defined for the other sections of this chapter.***

RFID tags and readers	
Risk:	There is no protection against unauthorized tampering with data on the chip.
Control:	The chip should be read only.
Finding:	**F4**: The chip is found to be read only.
Recommendation:	None

RFID tags and readers

Risk:	There is no way to check the authenticity of a chip.
Control:	The chip should have an authenticity checking mechanism.
Finding:	**F5**: The chip does not have an authenticity checking mechanism.
Recommendation:	Use RFID tags and readers that implement authenticity checking. This can be done with a public and private key scheme. Then, it might still be possible to clone the chip, but the authenticity of the chip can be checked by readers. In other words, clones can be detected.

Passport documents	
Risk:	The passport document does not have adequate security features.
Control:	The passport document should have adequate security features.
Finding:	**F6**: Legislation dictates certain requirements regarding what information should be in passport documents. These requirements are (also) represented in the form of a model, which prescribes a field for a stamp of the issuing organization. Also, signatures are prescribed, i.e. for modifications of the document. However, besides stamps and signatures, there are no requirements concerning security features of the document. All documents are printed by the PVV and have the same model. They are made of the same materials. The PVV uses paper with a UV-visible pattern.
Recommendation:	We recommend to define a set of adequate security features for the document and implement these in an all new document. Especially the the transponder number should be difficult to tamper with. For available techniques, we recommend to look at used techniques with human passport documents. It should be noted that when security features are added to the document, security measures regarding blank passports become increasingly important.

Data processing and storage

Risk:	No adequate measures in place to ensure data integrity of a database.
Control:	Adequate integrity checking should be used to ensure data integrity of a database.
Finding:	**F7**: There are no specific requirements from PVV regarding data processing and storage. Data processing and storage are handled separately by each passport issuing organization. Unfortunately, we could not investigate the situation further because of time constraints.
Recommendation:	Regulation of data processing and storage should be well defined and documented by PVV as the central controlling organization in the Netherlands.

Procedures	
Risk:	Not applicable
Control:	Not applicable
Finding:	Not applicable
Recommendation:	Not applicable

4.2.2 Accountability

Risk scenarios:

- ***Nobody can be held responsible for the security of the system.***
- ***Animal ownership cannot be determined.***
- ***Changes to the registration of animals cannot be traced.***

RFID tags and readers	
Risk:	Nobody can be held responsible for the security of RFID tags and readers.
Control:	Responsibility ('business owner') for security of RFID tags and readers should be well defined.
Finding:	**F8**: The RFID tags and readers must comply to ISO standards. This is dictated by EU legislation[1]. The PVV merely implements this legislation. So, the EU, as a legislator, is

	responsible for the (lack of) security of RFID tags and readers.
Recommendation:	Raise political awareness of the security of horse animal identification and registration. Furthermore, document security requirements in the EU legislation.

Passport documents	
Risk:	Nobody can be held responsible for the security of passport documents.
Control:	Responsibility ('business owner') for security of passport documents should be well defined.
Finding:	**F9**: The PVV is responsible for designing and printing the passport document. However, ultimately lawmakers and politicians are responsible, since PVV is essentially an organization that implements legislation.
Recommendation:	Raise political awareness of the security of horse animal identification and registration. Furthermore, document security requirements in the EU legislation.

Passport documents	
Risk:	Issuing and revoking of passport documents cannot be traced.
Control:	Issuing and revoking of passport documents should be adequately recorded and administrated.
Finding:	**F10**: Issuing and revoking of passport documents is recorded by the 31 passport issuing organizations. They have to keep an administration of all issued passports. The PVV website offers a possibility to look up the passport issuing organization associated with a certain transponder number. Auditing the factual administrations is outside the scope of the research.
Recommendation:	Take into account the process of issuing and revoking passport documents when auditing the passport issuing organizations.

Data processing and storage

Risk:	Nobody can be held responsible for the security of data processing and storage.
Control:	It should be clear who has responsibility for security of data processing and storage.
Finding:	**F11**: The passport issuing organizations are responsible. PVV requires that a minimum set of attributes of each animal is registered and stored for at least 35 years for a living animal, or at least 2 years after the death of an animal. The organizations have to submit animal identification number / transponder number combinations to the central database of PVV. For the rest, it is up to the issuing organizations how they handle data processing and storage.
Recommendation:	None

Data processing and storage	
Risk:	Changes to the contents of a database cannot be traced.
Control:	Changes to the database should be logged and hence traceable.
Finding:	**F12**: Data processing and storage are handled separately by each passport issuing organization. Unfortunately, we could not investigate the situation further because of time constraints. There are no specific requirements from PVV regarding data processing and storage.
Recommendation:	Regulation of data processing and storage should be well defined and documented by PVV, the central controlling organization in the Netherlands.

Procedures	
Risk:	Nobody can be held responsible for the security of procedures.
Control:	It should be clear who has responsibility for security of procedures.
Finding:	**F13**: The PVV is responsible for formalizing procedures in legislation and instructions. The issuing organizations have to adhere to these procedures. As a lot of procedures are based on

	European legislation that has to be adopted by national governments, politicians are ultimately responsible.
Recommendation:	Raise political awareness of the security of horse animal identification and registration.

Procedures	
Risk:	Deniable transaction: After the transfer of ownership, one party is able to deny the fact that he has made commitment, and hence want to reverse the process to re-obtain the ownership or not to admit that he was the previous/current owner of the horse.
Control:	Change of ownership should be clearly recorded.
Finding:	**F14**: Ownership is recorded in the passport document, which is also dictated by legislation. However, it is no legal proof of ownership.
Recommendation:	It can be expected that an animal owner wants to keep a legal proof of ownership (e.g. a document) always with him and store it in a safe place at home. This is not possible with the passport document, as it should always be kept near the animal. This is normally at a stable, but it should also be carried when the animal moves, e.g. to a race. It may not always be the case that the owner himself is the one that carries the passport document. Therefore, making the passport document also the legal proof of ownership would give rise to aforementioned practical problems. It is very well possible to document the proof of ownership (and a transfer of ownership) in a contract. However, this is not a very common practice. Horse organizations like stud books could inform the public more actively about the possibility to document the ownership of an animal. Also, the PVV, or another central organization, could set up an infrastructure (e.g. a database) that facilitates the recording of ownership of animals.

4.2.3 Authenticity

- ***Risk scenario: Animal identity is unauthentic***

RFID tags and readers	
Risk:	Impersonating a genuine tag by: –copying/cloning –plain read (lack of protection) –crypto attack –side channel attack –eavesdropping on the communication between tag and reader. –reading out a tag covertly (from a distance)
Control:	Protection technology should be used to prevent impersonating a genuine tag.
Finding:	**F15**: The tag is easy to copy or clone. There is no encryption or protection on the chip as the transponder number is not confidential. However, leaving the tag unprotected does open a window for other types of attacks. Figure 6 below shows a clone-attack of the chip carried out by us as an experiment on the widely used readers, for instance, by vets. We cloned the original glass tag to a re-programmable credit card type chip and let the personnel read it using the genuine reader. As can be seen in the figure, the difference between the original and the cloned chip cannot be determined. We ordered similar glass tags to the original tags but wrong chips were delivered. That's why we used a credit card type chip in the experiment. However, size and form of the chip do not matter so much in this case, as long as they are of the same type.
Recommendation:	Implement active authentication using asymmetric cryptography on the tag in order to be able to detect cloned chips. The same technique is also used in human ePassports[7].

Figure 6: Readout of a cloned animal RFID tag

RFID tags and readers	
Risk:	There is more than one tag with the same transponder number in the system.
Control:	There should be measures in place to prevent non-unique numbers in the system.
Finding:	**F16**: Transponder numbers that are registered with passport issuing organizations are checked against the central PVV database. This prevents non-unique transponder numbers being registered. However, it is still (theoretically) possible that there are two or more horse animals that have the same transponder number: Manufacturers can only ensure that within their product range the transponder is unique. Somehow, other manufacturers or individuals can produce chips with any transponder number as they want. However, the chance of two or more instances of the same transponder number interfering with each other is very low.
Recommendation:	None

Passport documents	
Risk:	Spoofing the identity of an animal with an existing, genuine passport document.
Control:	1) Refer to Controls for data integrity in paragraph 4.2.1. 2) Furthermore, animal features, i.e. drawings and biological features, should be well documented in the passport.
Finding:	**F17:** 1) Refer to findings of data integrity in paragraph 4.2.1. 2) Requirements for which information should be in the passport document are well defined in the legislation, in the form of a standard model. Issuing organizations adhere to this model. It is only possible to check online whether a certain identification number / microchip number combination is registered and at which issuing organization. It is not possible to obtain more information online, except for the Appaloosa stud-book[6]. It *is* possible to contact the issuing organization to obtain more information.
Recommendation:	1) Refer to recommendations for data integrity of passport documents in paragraph 4.2.1. 2) Make verifying the identity with the issuing organization easier, for example by means of a website. Make people, for example buyers of horses, aware that they can check with the issuing organization to verify the identity of an animal. Not only compare transponder numbers, but also check other identity attributes of the animal.

Passport documents	
Risk:	Obtaining a blank passport and creating a false identity with it.
Control:	Adequate security measures should be in place at the location(s) where the passports are printed and stored.
Finding:	**F18**: There are no requirements regarding blank passports mandated by means of legislation. This is the responsibility of the issuing organization. According to interviewed issuing organizations[8][9][10][11], they securely store and process blank passports, but there are no special procedures. This is neither the case at the PVV or at the printing company that prints the documents[12].

Recommendation:	Implement (basic) security measures regarding blank passport documents, especially at the printing company. When the passport document would be improved with security features, security regarding blank passports becomes much more important.

Passport documents	
Risk:	Altering a genuine passport to change the identity (i.e. breed) of the associated animal. Refer to paragraph 4.2.1.
Control:	Refer to paragraph 4.2.1.
Finding:	**F19**: Refer to paragraph 4.2.1.
Recommendation:	Refer to paragraph 4.2.1.

Data processing and storage	
Risk:	Not applicable
Control:	Not applicable
Finding:	Not applicable
Recommendation:	Not applicable

Procedures	
Risk:	An animal that is not intended for human consumption gets in the human food chain.
Control:	There should be an opt-out - not an opt-in -, for animals that are not intended for slaughter for human consumption, to protect food safety.
Finding:	**F20**: This is already implemented: When the owner of an animal doesn't note in the passport document that the animal is not for slaughter for human consumption, it will automatically be considered for slaughter. A stricter policy for medicines will apply accordingly.
Recommendation:	None

4.2.4 Authorization

- ***Risk scenario: Unauthorized adding, changing or removing of animal identities.***

RFID tags and readers	
Risk:	Unauthorized changing of the contents of the chip.
Control:	Contents of chip should not be changeable by an unauthorized person.
Finding:	**F21**: The chip is read-only glass tag. It is not possible to reprogram it. Therefore authorization is not applicable in this case.
Recommendation:	None

Passport documents	
Risk:	Unauthorized modifying of the passport.
Control:	It should be clear what modifications are allowed and by whom. Note: falsifying is covered in paragraph 4.2.3.
Finding:	**F22**: In the passport document it is clearly stated who can add certain information to the document. This regards mainly information to be added by a veterinarian doctor. The only piece of information that can be added by the owner or his/her representative is whether an animal is intended for slaughter for human consumption or not. However, this should be confirmed by the signature and name of a veterinarian.
Recommendation:	None

Data processing and storage	
Risk:	An unauthorized person changes contents of a database.
Control:	Implement authentication and an adequate access control policy.
Finding:	**F23**: Data processing and storage are handled separately by each passport issuing organization. Unfortunately, we could not investigate the situation further because of time constraints.

Recommendation:	Not applicable

Procedures	
Risk:	Unauthorized first registration of an animal.
Control:	Application for registration should be verified by an independent person, like a veterinarian. The animal should be physically identified by this person. The transponder number of the implanted chip should be verified. Also, only one chip should be associated to the animal. Therefore it must be checked whether there is already a chip implanted, and if there are signs of a previously implanted chip. The identity of the person who implants the chip should be verified.
Finding:	**F24**: There is a formalized protocol[4] for implanting chips and applying for registration. According to this procedure, only veterinarians or 'passport advisers' that are recognized by the passport issuing organization may implant the chip. They have to check for already implanted chips and signs of removal of a previously implanted chip. There is no requirement on the application form[13] for a copy of an identification document of the person who implants the chip.
Recommendation:	Require a copy of a valid identification document of the person who implants the chip.

Procedures	
Risk:	Unauthorized unregistering or not unregistering of an animal (e.g. when an animal dies).
Control:	When an animal dies, this should be properly registered by the passport issuing organization. The passport document should be returned to the passport issuing organization or the PVV. The transponder number should be revoked. The RFID tag should be destroyed.
Finding:	**F25**: When a dead animal is processed by a destruction company, the animal owner himself is responsible for returning

	the passport document. He can choose to have it returned to him after being physically invalidated. When a dead animal is slaughtered, the abattoir owner is responsible for confiscating the passport document and returning it to PVV, who in turn will send it back to the passport issuing organization it belongs to. The abattoir owner is also responsible for removing and destroying the RFID tag. When the tag cannot be found, it is not allowed to slaughter the animal for human consumption, because of food safety.
Recommendation:	None

Procedures	
Risk:	Unauthorized reregistering (i.e. when a new passport or RFID chip is issued) of an animal.
Control:	It should be sufficiently clear that the old passport document is missing or that the old RFID tag is not functioning anymore. The identity of the applicant should be clear.
Finding:	**F26**: An applicant for a duplicate or replacing passport document has to answer a list of questions about the reason for the loss of the original passport. He should also inform the police of the loss. However, we found that in at least one case, the police didn't want to take a statement about a lost passport document and referred to the local town hall[14]. Whether an applicant has to send a copy of his/her identification document along varies: the FPS stud-book does not[19], while the AVS stud-book does[20].
Recommendation:	Always require a copy of an identification document of the applicant when issuing a duplicate or replacing passport document.

4.3 Availability

- ***Risk scenario: Identification and/or registration of animal identities is (temporarily) not possible.***

RFID tags and readers	
Risk:	Tag gets permanently disabled by: –tag removal tag destruction –KILL command (a special command implemented in certain RFID chips) –normal 'wear and tear'
Control:	Tags should not be easily removable or broken. The tag should be strong enough to last working for the at least the ISO standardized life time of a tag which is 30 years[15].
Finding:	**F27**: For impersonation it can be interesting to remove or disable the original chip and to implement a second, cloned tag. It is not easy to remove the tag from horse once implanted. The horse can be seriously hurt if the tag is taken out by improper operation. Disabling an RFID chip is possible using an electromagnetic pulse [16]. Tags with a normal form factor can easily be 'zapped' using for example a modified external camera flash unit like the one in figure 7. Tests reveal that we can indeed 'zap' chips with a normal, credit card size, form factor. However zapping glass tags failed with the tested equipment. However, we believe that it is possible using modified equipment. Because of time constraints we weren't able to test this. The tag is not programmable, so hence there is no KILL command. There are cases that defection of the tag can happen, but this does not occur often: one manufacturer indicated a figure of 1 to 2 cases per 1000 tags[3].  *Figure 7: Flashing device*
Recommendation:	There is no simple fix for protecting against 'zapping'. This risk is by design.

RFID tags and readers	
Risk:	Tag gets temporarily disabled by: –passive interference –active jamming –relay attack
Control:	A reader should be able to identify individual chips when there are multiple chips presented at the same time. The influence of jamming should be minimized.
Finding:	**F28**: A reader does not give a read out when multiple chips are presented. Instead of an error message telling that multiple tags are present, it displays the message "no tag presented". We could not test jamming, as we didn't have a jamming device to our disposal.
Recommendation:	Consider implementing anti-collision technology into the RFID tags and readers and adding this to the ISO standard.

Passport documents	
Risk:	The passport gets damaged due to poor material quality.
Control:	The document quality should be adequate.
Finding:	**F29**: We have found that the document quality is adequate. For most horses the passport document will not be prone to heavy wear and tear like a passport for humans could be.
Recommendation:	None

Passport documents	
Risk:	Someone gets hold of a passport document that does not belong to him/her due to: – theft – accidental loss

	Note: See also the risk Unauthorized reregistering (i.e. when a new passport or RFID chip is issued) of an animal in paragraph 4.2.
Control:	There should be a designated and sufficiently secure place where the passports are stored. The passport should not be taken away from there unless there's a reason for it. There should be an adequate procedure to obtain a replacement passport.
Finding:	**F30**: Legislation dictates that the passport should always be kept in the vicinity of the horse. We found this was the case at the stable that we visited[14]. There is a formal procedure to obtain a duplicate passport document at the issuing organization when identification of the animal is still possible by means of an animal identification number or transponder number. When animal identification is no longer possible, a new, replacing passport is issued. In particular the latter may be troublesome[14] because it must be plausible that the old document is really lost.
Recommendation:	It is recommended to passport holders to make a copy of the page that contains the identification number and transponder number of an animal to prevent delay when applying for a replacing passport.

Data processing and storage	
Risk:	The information in the database becomes unavailable, i.e. due to: - dos attack on the database server - hardware failure - a disaster, like a fire - accidental removal of some or all information (i.e. by a junior system administrator) - network failure
Control:	The availability should comply to what is agreed in the SLA.
Finding:	**F31**: Data processing and storage are handled separately by each passport issuing organization. Unfortunately, we could not investigate the situation further because of time constraints.
Recommendation:	Not applicable. But in general, we recommend the organizations to choose a good hosting service provider if their database is

	available on-line. If not, security updates should be regularly applied. Disaster plan and backup plan should be well defined and strictly followed.

Procedures	
Risk:	Not applicable
Control:	Not applicable
Finding:	Not applicable
Recommendation:	Not applicable

5 Conclusions & discussion

5.1 Conclusions

We will draw conclusions from our research by revisiting the our research questions:

What general security requirements should the system meet?

We used the CIA model to define these general security requirements. It was found that from the three cornerstones that this model is devised of, in particular integrity is important in the system of horse identification and registration. Lack of integrity opens up the possibility to spoof an identity.
Confidentiality is less important, as the information in the system is mostly not (very) confidential.
The same holds true for Availability, as verifying of the identity is mainly done 'off line' by comparing the transponder number in the horse passport with the transponder number on the RFID tag.

What risks is the system imposed to?

The RFID tags are read only and the transponder number on it can therefore not be changed. However, cloning of a tag is easy. The RFID tags and readers do not use a protection mechanism to detect clones. It is possible to impersonate an animal by making a clone of the implanted tag, and implanting it in another animal. An already implanted tag may be disabled (refer to paragraph 4.3).
Passport documents have very few security features. Fraudsters could easily make false documents.
Data processing and storage is mostly done locally at the location of the 31 passport issuing organizations. As a result, many people have (write) access to these data, which poses a security risk.

How can the security of the system be improved?

To be able to detect clones of RFID tags, we recommend to implement an authenticity checking mechanism into the RFID tags and readers. If this is not possible, we recommend to implement some sort of central online checking possibility (e.g. a website) to be able to look up full information about a certain animal. This would help mitigate 'off line' fraud. Now it is only possible to look up the passport issuing organization that is associated with a certain transponder number.

Implementing (more) security features in the passport document would make forging and altering of passport documents harder. We recommend defining a set of adequate security features that make it more difficult to successfully forge a document and that make it easier to detect forgeries. Furthermore, we recommend to formalize these security features and to implement the new security features in an all new document.

Finally, we recommend considering setting up a central organization to carry out the system of identification and registration of horse animals, instead of the current 31 passport issuing organizations.

5.2 Discussion

From our research, we concluded that the current system of horse animal identification and registration has shortcomings.
Now, one could argue that a (more) secure system is not worth the costs. If properly calculated, this could be a valid statement when it concerns information security in an organization. However, in the system for horse animal identification and registration, damages as a result of insecurity would be imposed on individuals (i.e. a buyer of a horse) and not a (large) organization. An individual does not have the choice to weigh security against costs. He/she would have to go to court and sue the fraudster, and perhaps the PVV too. Then, it may turn out that the PVV cannot be held liable, because it is only implementing legislation made by politicians.
Therefore, politicians also play an important role in the security of the system and in the decision making to improve this security.

Furthermore, it must be noted that for very expensive horses and connoisseurs of horses, the risk of fraud in the system of horse animals is limited, because connoisseurs 'know' the horse and may use DNA checking techniques. Fraud with the system is most attractive in cases of 'middle-class' horse animals and/or involving buyers that are not experienced.

It is suggested to further research the recommendations to improve the security of the system that are made in this report.

References

[1] *EC regulation 504/2008*, June 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:149:0003:0032:EN:PDF

[2] *Verordening identificatie en registratie van paardachtigen (PVV)*, 2009, http://www.pve.nl/wdocs/dbedrijfsnet/up1/ZumrasbIE_Verordening_I_R_paardachtigen_2009.doc-20090622154652.pdf

[3] Survey answered by Virbac Nederland B.V., February 2010

[4] *Besluit protocol implanteren transponder I&R paardachtigen (PVV)*, 2009, http://www.pve.nl/wdocs/dbedrijfsnet/up1/ZumrasbIM_Bsl_protocol_implanteren_transponder_I_R_paardachtigen__PVV__2009.doc-20090622154846.pdf

[5] *I&R database*, February 2010, http://www.pve.nl/pve?waxtrapp=szhtBsHsuOpbPREcBhBaBL&context=hfMsHsuOpbPREY

[6]*Website Appaloosa Stud-book*, January 2010, http://www.appaloosa-stamboek.com

[7]*Wikipedia: Biometric passport*, February 2010, http://en.wikipedia.org/wiki/Biometric_passport

[8] Survey answered by Merens Stud-book, January 2010

[9] Survey answered by Arabische Volbloedpaarden Stud-book, January 2010

[10] Survey answered by KFPS stud-book, January 2010

[11] Survey answered by Welsh Pony & Cob Vereniging, January 2010

[12] Survey answered by Productschap Vee en Vlees, February 2010

[13] *AANVRAAGFORMULIER PASPOORT PAARDACHTIGEN (PVV) 2009 (*application form for passport document), February 2010, http://www.paardendierenarts.nl/uli/?uli=AMGATE_7364_102_TICH_L891557778

[14] Interview with stable, January 2010

[15] ICAR Subcommittee on Animal Identification, *Information about the use of country code, manufacturer code and product code ISO TC23\SC19\WG3 'Animal Identification',* September 2008, http://www.wsava.org/PDF/2008/Misc/2008_Manufacturer_CountryCode.pdf

[16] Aikaterini Mitrokotsa, Melanie R. Rieback and Andrew S. Tanenbaum *Classification of RFID Attacks*, 2008

[17] Peeger C.F., *Security in Computing*, 1989

[18] Russell D., *Computer Security Basics*, 1991

[19] International Organization for Standardization iso: *ISO/IEC 27002: Code of*

practice for information security management, 2005

[20] *Aanvraagformulier tot uitgifte van Duplicaat of Vervangend Paardenpaspoort,* www.fps-studbook.com%2Fsrc%2Fcontent%2Fcontent.asp%3Flink%3DL0097%26taal%3D1&ei=Q5xyS9-VL43B-Qba_IgV&usg=AFQjCNGVeItjhMZFq7SJiIlWlSieU5JvHw&sig2=OdEAvGMV2h1WyEc3tmxi2w, February 2010

[21] *AANVRAAGFORMULIER DUPLICAAT PASPOORT PAARD (PVV) 2009*, www.avsweb.nl%2FSubcategorieen%2FSecretariaat%2FFormulieren%2FForms_Aanvraag_Duplicaat_Paspoort.pdf&ei=Q5xyS9-VL43B-Qba_IgV&usg=AFQjCNF6f9b9VaDldtRS1ultvhYnLV-qyg&sig2=HonHeNhfuCfFvUuTRCDXzA

Appendix A: RFIDIOt logs

RFIDIOt was used to read and write to RFID tags during this research. It can be downloaded from http://www.rfidiot.org

```
##########################################################
## cloned on card
##########################################################
fx160-02:~/Documents/rfid$ sudo ./readlfx.py
establishcontext failed: -7fefffe3
*** Warning - no pyscard installed or pcscd not running
readlfx v0.1l (using RFIDIOt v1.0a)
 Reader: ACG LFX 1.0  (serial no: 08070045)

Card ID: ZXXXXXXXXXXXXXXXX
Tag type: EM 4x05 (ISO FDX-B)

Application Identifier:  8000
Country Code:  528 (Netherlands)
National ID:  XXXXXXXXXXXX
 Checking for Q5

   Native - UNIQUE ID: XXXXXXXXXXXXXXXX

##############################################
## from original glass tag
##############################################
fx160-02:~/Documents/rfid$ sudo ./readlfx.py
establishcontext failed: -7fefffe3
*** Warning - no pyscard installed or pcscd not running
readlfx v0.1l (using RFIDIOt v1.0a)
 Reader: ACG LFX 1.0  (serial no: 08070045)

Card ID: ZXXXXXXXXXXXXXXXX
Tag type: EM 4x05 (ISO FDX-B)

Application Identifier:  8000
Country Code:  528 (Netherlands)
National ID:  XXXXXXXXXXXX
 Checking for Q5

   Native - UNIQUE ID: XXXXXXXXXXXXXXXX
```

```
##########################################################
## writing to the original glass tag: failed with block 7
##########################################################
fx160-02:~/Documents/rfid$ sudo ./fdxbnum.py XXXXXXXXXXXXXXXX WRITE
establishcontext failed: -7fefffe3
*** Warning - no pyscard installed or pcscd not running
fdxbnum v0.1e (using RFIDIOt v1.0a)
 Reader: ACG LFX 1.0  (serial no: 08070045)

Decode:

Application Identifier:  8000
Country Code:  528 (Netherlands)
National ID:  XXXXXXXXXXXX
```