



Horse-ID

**Security of Horse Animal Identification &
Registration in The Netherlands**

SNE Research Project 1

Laurens Bruinsma

Vic Ding

Agenda

- Introduction
- Research question
- System overview
- Research methodology
- Findings
- Conclusion
- Recommendation
- Demo
- Ending

Introduction (1)

- Implanted RFID tag + passport
- No chip in passport!
- Mandatory
- Based on EU legislation
- Not only horses, but also other animals, like dogs/cats

02/11/10

Introduction (2)



02/11/10



Introduction (3)



Introduction (4)

Goals of the system:

- Preventing / discouraging fraud in sports and trade
- Preventing / discouraging theft
- Keeping record of medical treatment
- Food safety → public health

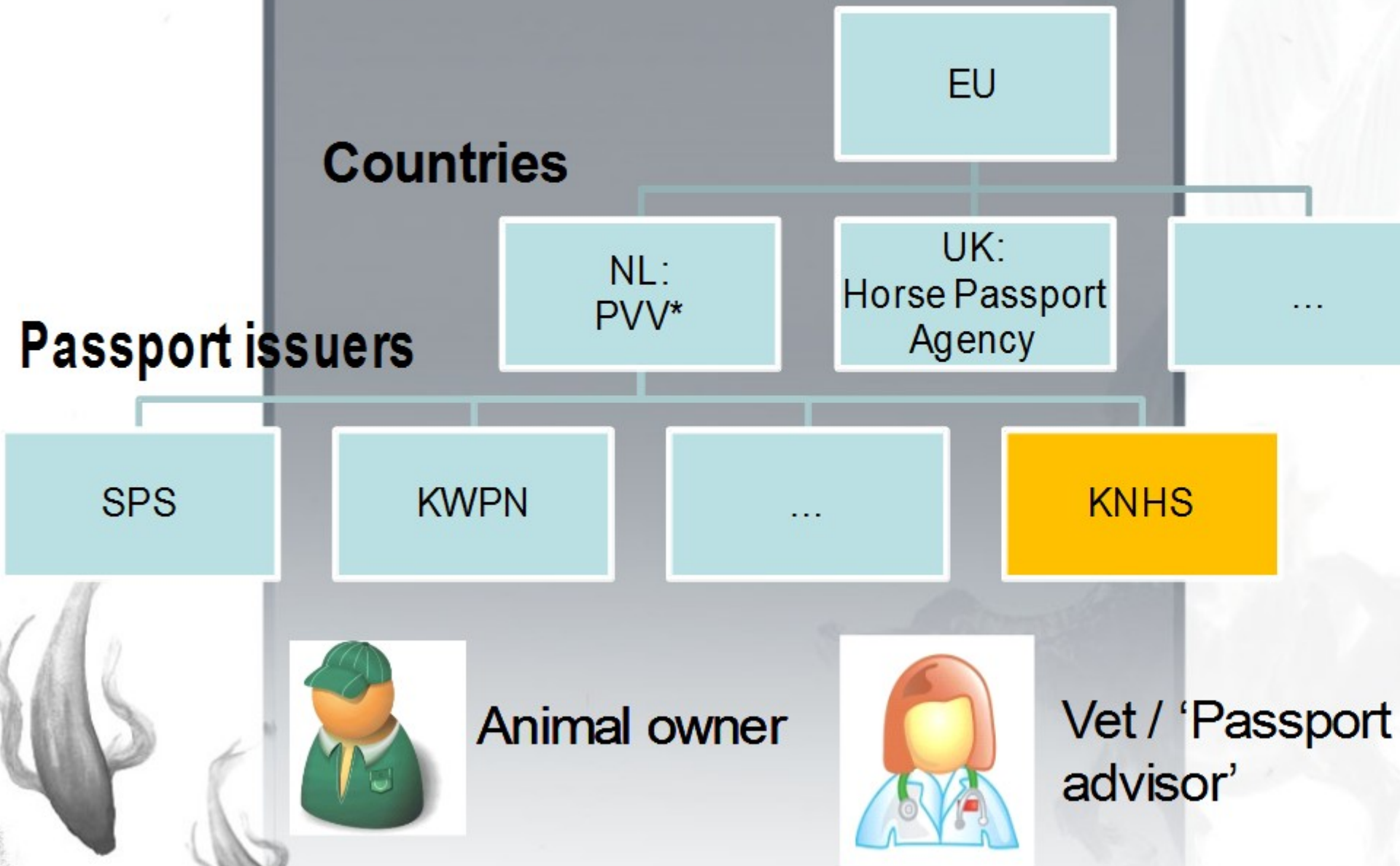


= \$\$\$

Research Questions

- *What general requirements should the system meet?*
- *What risks is the system imposed to?*
- *How can the security of the system be improved?*

System Overview (1)





Ve
"Het N
Fjord
Sta



Koninklijke Vereniging
"Het Nederlandse
Trekpaard
en De Haflinger"



Welsh
mboek

ng

K

System Overview (2)

- Reader/tag
 - bio-glass or biopolymer encasing
 - LF fdx-B reader
 - ISO 11784 & 11785
- Tag code structure
 - 3 digit country code
 - 1 digit user group / manufacturer
 - 2 or 3 digit manufacturer pseudo-code
 - 8 or 9 digit unique code

Example : 5280000000000000

Risk Scenarios

- Impersonation
 - cloning RFID tag
 - false passport
- Tag gets permanently disabled
- Tag/reader gets temporarily disabled

Research Methodology (1)

- General, high level requirements: CIA model
- Risk analysis
 - RFID tags & readers
 - Passports
 - Procedures
 - Data processing & storage
- Formulating controls
- Field research of current situation
- Recommendations

Research Methodology (2)



02/11/10

Research Methodology (3)



02/11/10

15

Research Methodology (4)



02/11/10

16





Findings: Passports (1)

Scenario: Impersonation

- **Passport:**
- Document security
 - UV visible pattern on paper
 - stamps
 - signatures
 - bar code stickers RFID tag code

Findings: Passports (2)

IDENTIFICATIEDOCUMENT
REGISTRATION CERTIFICATE/CERTIFICAT D'ENREGISTREMENT/EINTRAGUNGSSCHEIN

Naam Name/Nom/Name Levensnummer Identification number Numéro d'identification Lebensnummer Transpondernummer Microchip number Numéro du transpondeur Mikrochip Nummer Geslacht Sex/Sexe/Geslacht Stamboek/Ras/Stud-Book L'association d'élevage/Zuchtverband Type/Type/Type/Typ Vader/Sire/Père/Vater Moeder/Dam/Mère/Mutter Moeders vader Sire of Dam/Père de Mère/Mutters Vater Geboortedatum, -plaats Date of birth, place of birth Date de naissance, place de naissance Geburtsdag, Geburtsort Lidnummer: Fokker(s)/1e eigenaar, Breeder/Naisseur/Züchter		Kleur: Colour/Robe/Farbe  Certificaat van oorsprong geldig vanaf: door: Origin certificate validated on: by: Certificat d'origine valide le: par: Certifikat von Ursprung, gültig ab: betr.:  Naam van de bevoegde instantie: Name of the competent authority: Nom de l'autorité compétente: Name der befugte zuständigen Stelle: Adres: Address: Anschritt: Telefoonnummer: Telephone number: No. de telephone: Telefonnummer: Telefaxnummer: Fax number: No. de telecopie: Telefaxnummer: E-mail adres: 
---	---	--

1

Findings: Procedures

Scenario: Impersonation

Procedures:

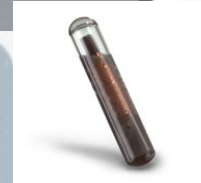
- no security measures blank passports
- no copy of ID applicant needed
- passports of dead horses not always returned

Findings: RFID (1)

Scenario: Impersonation

RFID tag:

- no protection built in chip
- eavesdropping easy but not interesting
- covert read out: read distance varies
- cloning easy



Findings: RFID (2)

Scenario: Tag gets permanently disabled

- difficult to remove
- “flashing” is possible
- different size, different antenna
- glass tag → more energy required



Findings: RFID (3)

Scenario: Tag/reader gets temporarily disabled

- Interference / Collision
 - no read out
- Jamming
- Relay attack
 - possible but not necessary

Conclusions

- Reader/tag
 - reader, functionally poor
 - tag, insecure
- Document
 - Poor document security
 - Poor security for blank passports
- Data processing and storage
 - mostly unknown
 - No easy check of identity for public
- Procedures
 - On paper, but enforcement troublesome
 - Many individual organizations

Recommendations (1)

General:

- Consider central organization for passport issuing and registration

RFID tags & readers:

- Authentication of chip
 - Using public/private key pair + challenge/response
 - Protection against cloning
- Anti-collision technology

Recommendations (2)

- Procedures
 - audit passport issuing organizations regularly
 - fine an owner that doesn't return passport of dead horse
 - verify identity of applicant for:
new or replacing passport

Recommendations (2)

- Passport
 - implement (basic) security features
 - security measures blank passports
- Data processing & storage
 - online database with full information on identities

Demo

RFIDIot.org

- Open source
- Support a large number of devices

`./readlfx.py`

- Read out the card id (animal ID)

`./fdxnum.py`

- Decompensate a given ID, to national level
- Write the given ID to the tag

02/11/10

