Integration of the New German ID-Card (nPA) in Enterprise Environments

Technics – Prospects – Costs - Threats

Troopers 2011

BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE
PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE

T22000129

Name/Surname/Nom
MUSTERMANN
GEB. GABLER

Vornamen/Given names/Prénoms
ERIKA

Geburtstag/Date of birth/Date de naissance
12.08.1964

Staatsangehörigkeit/Nationality/Nationalité
DEUTSCH

Geburtsort/Place of birth/Lieu de naissance
BERLIN

Gültig bis/Date of expiry/Date d'expiration
31.10.2020

938568

Unterschrift der Inhaberin/des Inhabers - Signature of bearer - Signature de la titulaire/du titulaire

Mustermann

Common Criteria Protection Profile

Electronic Identity Card (ID_Card PP)

Common Criteria

BSI-CC-PP-0061

Approved by the
Federal Ministry of Interior

Version 1.03, 15th December 2009

By Friedwart Kuhn & Michael Thumann

Agenda

- **Introduction**
- **The New German ID-Card (nPA) – Technicl Overview**
  - Functions
  - Architecture
  - Supporting Background Infrastructure
- **Enterprise Integration of the nPA**
  - Szenarios
  - Qrganizational Requirements
  - Technical Requirements
  - Risks
  - Recommendations

Introduction

Introduction

- **Strong authentication continues beeing one of the most important security issues & goals and gains even more importance if services move to the cloud.**
  - It will be one of the few things ou can and should control ;-)

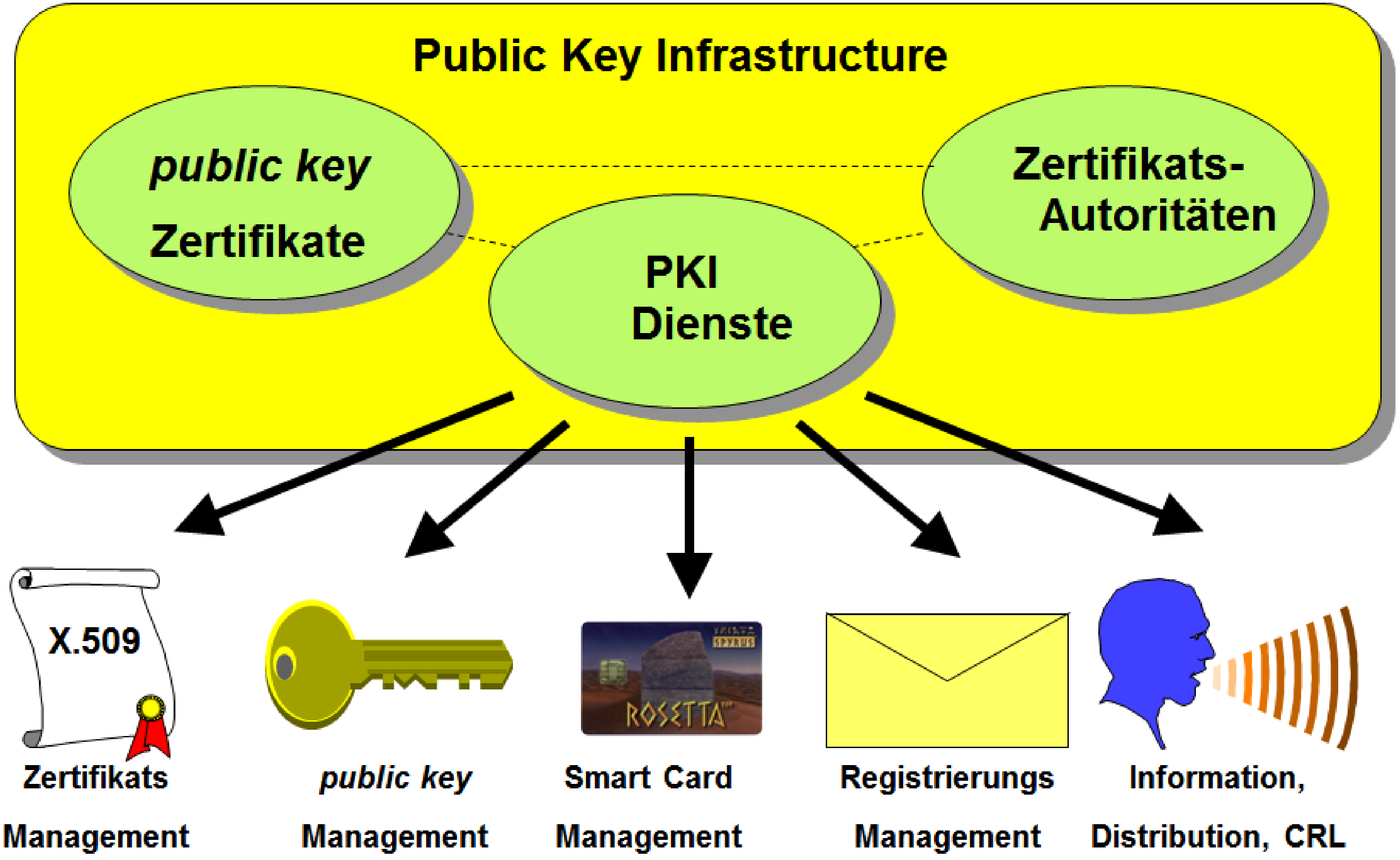
- **Strong authentication is achieved best with a certificate on a smartcard.**

- **In enterprise environments, this is done by implementing and running a PKI.**

Introduction

- **10 Requirements for Running a PKI**
  - Availability of the Components of a PKI
  - Identification and Authentification Processes & Services
  - Integrity of all Components and Processes
  - Scalability and Flexibility
  - Key-management
  - Certificate-Suspension, -Revocation and -Validation Management
  - Management of Responsibility
  - Traceability
  - Documentation
  - Compliance

Introduction



Introduction

- **Now imagine…**
  - Complex PKI infrastructure is completly run (for you ;-) by the government…
  - Processes and components are certified and will stay certified and you even don´t have the hassle with that…

- **Is this possible…?**

The New German ID Card
Technical Overview

BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE
PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE

T22000129

Name/Surname/Nom
MUSTERMANN
GEB. GABLER

Vornamen/Given names/Prénoms
ERIKA

Geburtstag/Date of birth/ Date de naissance
12.08.1964

Staatsangehörigkeit/Nationality/ Nationalité
DEUTSCH

Geburtsort/Place of birth/Lieu de naissance
BERLIN

Gültig bis/Date of expiry/ Date d'expiration
31.10.2020

938568

Unterschrift der Inhaberin/des Inhabers - Signature of bearer - Signature de la titulaire/du titulaire

Terminology, Range of Functions, Architecture

Terminology

- **ICAO International Civil Aviation Organization**
  - ICAO 9303 (part 1 – Specs for Machine Readable Travel Documents)
- **nPA /ePA New German ID Card**
  - „Neuer /elektronischer Personalausweis“

Terminology

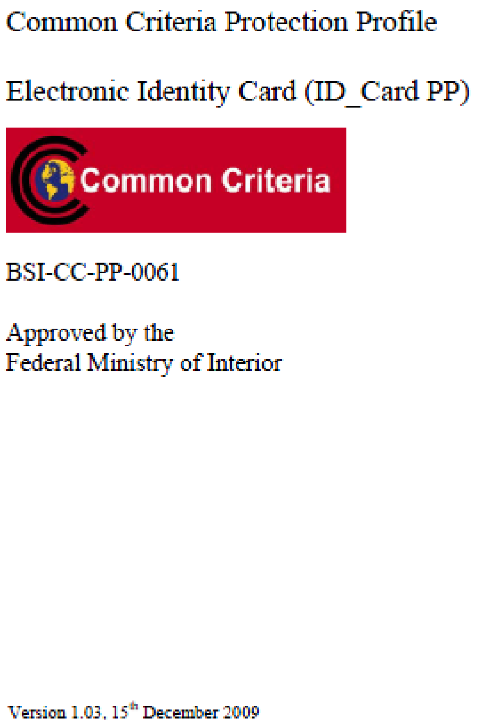
- **Terminal Card Reader**
  - Local card reader, card terminal of a service, inspection system

- **Inspection System**
  - Technical system used by an official authority and operated by a governmental organisation

- **QES Qualified Electronic Signature**
  - Electronic signature in accordance to the Act on Digital Signature [SigG] and the Signature Ordinance [SigV]

General Information

- **nPA**
  - ID-1
  - Card Body: Polycarbonate
  - RFID-Chip (compliant with ISO 14443)
    - Working range: 3,5 cm max
  - CC certification (EAL4+)
  - Compliant to TR-03110
    - Advanced Security Mechanisms for Machine Readable Travel Documents



Common Criteria Protection Profile

Electronic Identity Card (ID_Card PP)

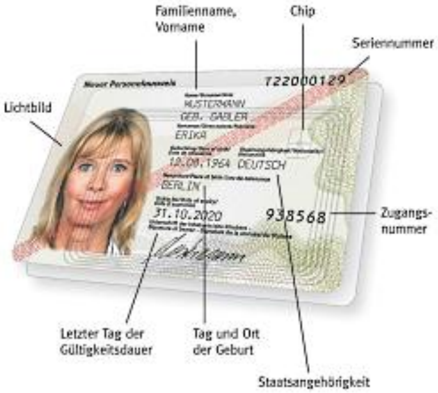
Common Criteria

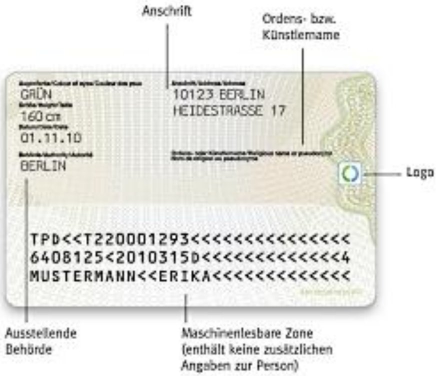
BSI-CC-PP-0061

Approved by the
Federal Ministry of Interior

Version 1.03, 15th December 2009

Data on the nPA





Secrets of the nPA

- **CAN**
  - The Card Access Number (CAN) is a short password that is printed or displayed on the document.
- **PIN**
  - The Personal Identification Number (PIN) is a short secret (6 numbers) password that SHALL be only known to the legitimate holder of the document.
- **PUK**
  - The PIN Unblock Key (PUK) is a long secret password that SHALL be only known to the legitimate holder of the document.
- **MRZ-Password**
  - The MRZ-Password is a secret key that is derived from the machine readable zone and may be used for both PACE.

nPA – Range of Functions

- **Physical Functions**
  - Visual /sight check for official identification
  - Tactile attributes

- **Electronic Functions**
  - nPA-Smartcard provides three applications for *official* and *commercial /private* use:

  - **ePass**(port)
  - **eID**
  - **eSign**

nPA – Functions **ePass**

- **ePass application** (required)

nPA

  - contains user data (incl. biometric) as well as data needed for authentication (incl. MRZ), intended to be used by authorities as a MRTD
  - Exclusive for Authenticated Inspection Terminals
    - TR-03127, 3.2.1
  - Inspection System (TR-03127)
    - Has **reading** access on MRZ data and the facial image
    - With corresponding rights access to biometric data

nPA – Functions **eID**

- **eID application** (optional)

  - For commercial (eBusiness) and official (eGovernment) use
    - Official use example: address changes at a local authority, car registration
    - Commercial use example: (certified) online shops
  - Provides (online) identity information
  - On (online) authentication the rights are defined, to which of the stored user data access is granted (via authorization certificate)

nPA – Functions **eSign**

- **eSign application** (optional)
  - Provides qualified electronic signature (QES) via qualified electronic (X.509) certificate
  - For commercial (eBusiness) and official (eGovernment) use
    - Official use: Announcement for trade- and business register (since 2010 only with electronic qualified signature)
    - Commercial use: Signing of PDFs (f. ex. electronic bill), long-time archiving of electronically signed documents (f. ex. with ArchiSig)

nPA Terminal Types

- **(E)IS (Electronic) Inspection System**
  - Official domestic /official foreign
    - Contains (cv-) certificate to prove identity

- **Authentication Terminal**
  - Official domestic or commercial
    - Contains (cv-) certificate to prove identity

nPA Terminal Types

- **Confirmed Signature Terminal** (nPA Card Reader)
  - For generating a QES
    - Contains (cv-) certificate to prove identity
  - Reader exampel: Reiner SCT RFID Komfort

nPA Terminal Types

- **Unauthenticated Terminal**
  - No Terminal or Chip authentication is required for certain administrative operations performed locally by the card holder
  - Reader exampel: Reiner SCT RFID Standard

nPA Card Reader Types

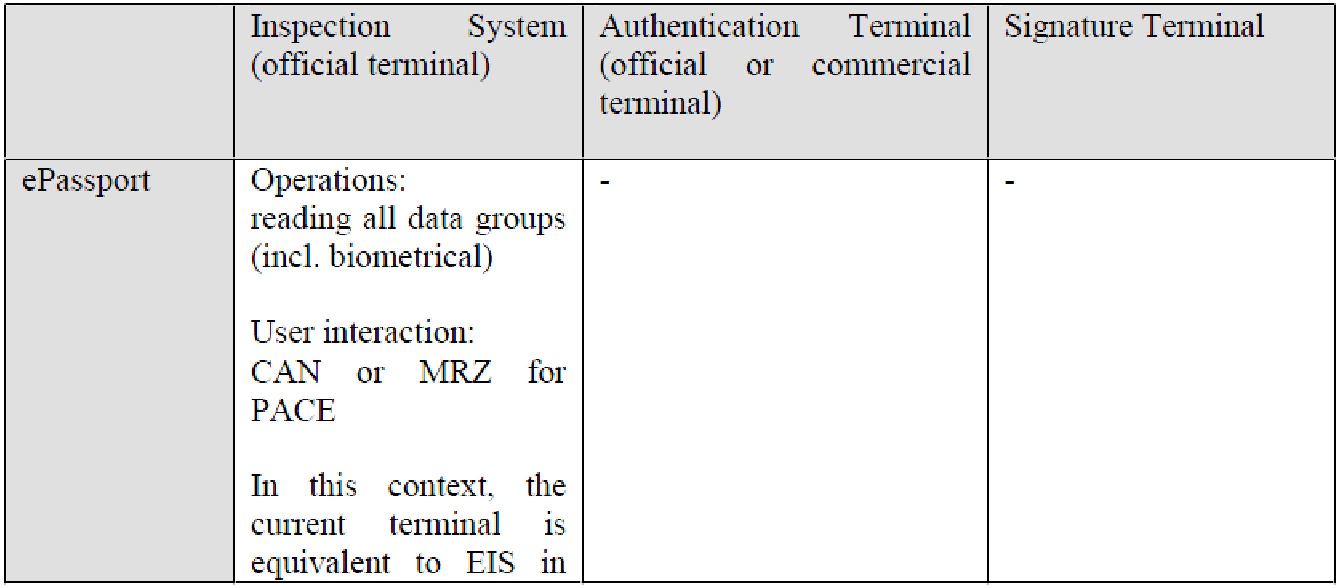
- **Reader of category "basis" = Kat-B**

- **Reader of category "standard": Kat-S**

- **Reader of category "komfort": Kat-K**

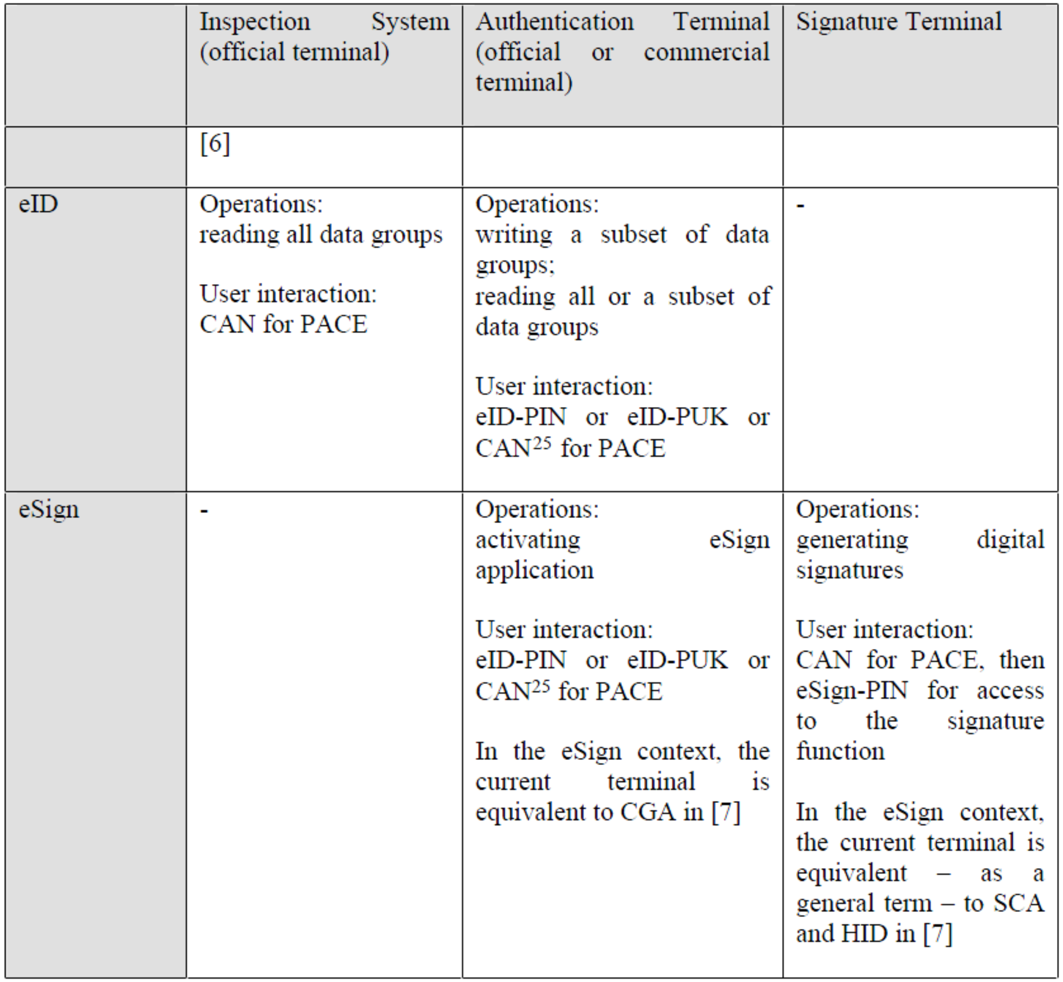
nPA Card Apps. vs. Terminal Types

- **See CC certification of nPA [PP-0061]**



	Inspection System (official terminal)	Authentication Terminal (official or commercial terminal)	Signature Terminal
ePassport	Operations: reading all data groups (incl. biometrical) User interaction: CAN or MRZ for PACE In this context, the current terminal is equivalent to EIS in	-	-

nPA Card Apps. vs. Terminal Types



	Inspection System (official terminal)	Authentication Terminal (official or commercial terminal)	Signature Terminal
	[6]		
eID	Operations: reading all data groups User interaction: CAN for PACE	Operations: writing a subset of data groups; reading all or a subset of data groups User interaction: eID-PIN or eID-PUK or CAN[25] for PACE	-
eSign	-	Operations: activating eSign application User interaction: eID-PIN or eID-PUK or CAN[25] for PACE In the eSign context, the current terminal is equivalent to CGA in [7]	Operations: generating digital signatures User interaction: CAN for PACE, then eSign-PIN for access to the signature function In the eSign context, the current terminal is equivalent – as a general term – to SCA and HID in [7]

nPA Communication Protocols

- **Password Authenticated Connection Establishment (PACE)**

- **Extended Access Control (EAC)**

nPA Communication Protocols

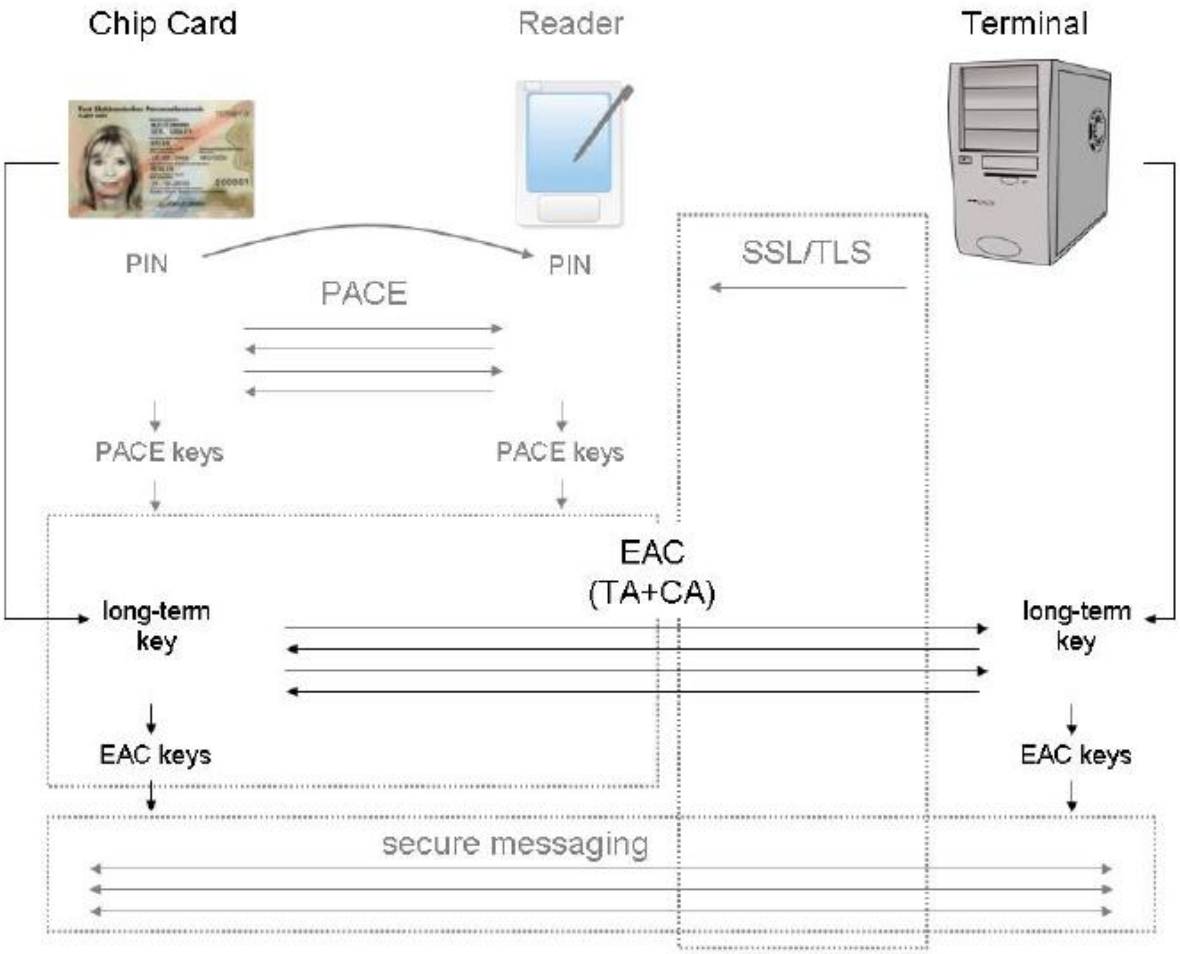
- **PACE [TR-03110]**
  - Password Authenticated Connection Establishment (TR-03110)
  - PACE is a password authenticated Diffie-Hellman key agreement protocol that provides explicit authentication of the MRTD chip, confidentiality and integrity of the communication.
  - PACE (otherwise like SPEKE) has the following attributes
    - not patented
    - formal (mathematical) security proof
  - PACE uses
    - ECKA 256 for key agreement; AES 128 CBC-Mode for encryption; AES 128 CMAC for Integrity

nPA Communication Protocols

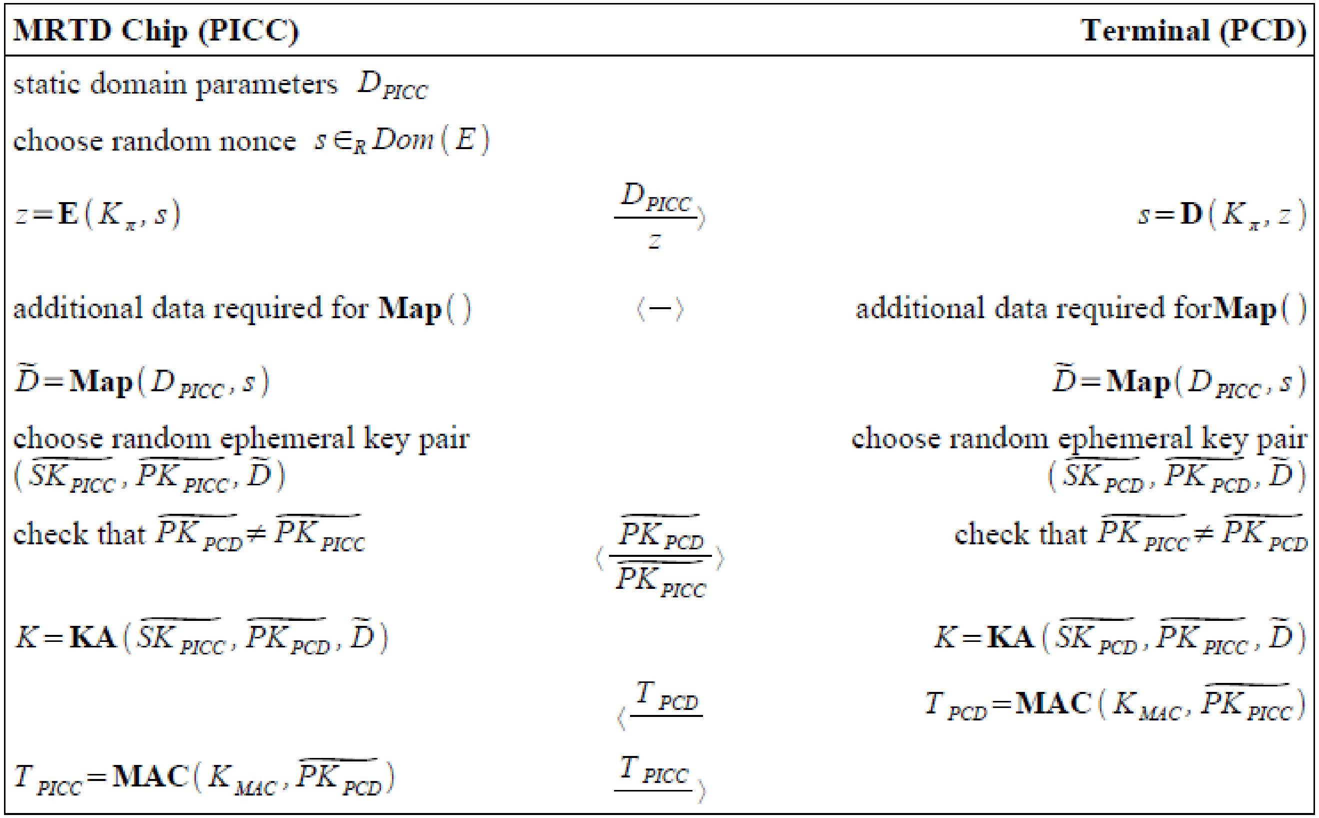
- **Extended Access Control (EAC) [TR-03110] is a protocol suite for MRTDs. Relevant for the nPA are:**
  - Terminal Authentication
    - Is a challenge response protocol that provides explicit unilateral authentication of the terminal.
    - All messages between terminal and chip are transmitted compliant to Secure Messaging [ISO 7816 – 4] using session keys derived from PACE or Chip Authentication.
  - Chip Authentication
    - Is an ephemeral static key-based Diffie-Hellman key agreement protocol that provides confidentiality and integrity in communication and unilateral authentication of the MRTD chip.
    - Used algorithms: ECKA 256 for key agreement; AES 128 CBC-Mode for encryption; AES 128 CMAC for Integrity.

nPA Communication Protocols

- **PACE + EAC overview [SecAna_EAC]**



nPA Communication Protocols – PACE [TR03110], p.33



MRTD Chip (PICC)		Terminal (PCD)
static domain parameters D_{PICC}		
choose random nonce $s \in_R Dom(E)$		
$z=\mathbf{E}(K_\pi, s)$	$\xrightarrow[z]{D_{PICC}}$	$s=\mathbf{D}(K_\pi, z)$
additional data required for **Map**()	$\longleftrightarrow$	additional data required for**Map**()
$\tilde{D}=\mathbf{Map}(D_{PICC}, s)$		$\tilde{D}=\mathbf{Map}(D_{PICC}, s)$
choose random ephemeral key pair $(\widetilde{SK}_{PICC}, \widetilde{PK}_{PICC}, \tilde{D})$		choose random ephemeral key pair $(\widetilde{SK}_{PCD}, \widetilde{PK}_{PCD}, \tilde{D})$
check that $\widetilde{PK}_{PCD} \neq \widetilde{PK}_{PICC}$	$\xleftarrow{\widetilde{PK}_{PCD}}$ $\xrightarrow{\widetilde{PK}_{PICC}}$	check that $\widetilde{PK}_{PICC} \neq \widetilde{PK}_{PCD}$
$K=\mathbf{KA}(\widetilde{SK}_{PICC}, \widetilde{PK}_{PCD}, \tilde{D})$		$K=\mathbf{KA}(\widetilde{SK}_{PCD}, \widetilde{PK}_{PICC}, \tilde{D})$
	$\xleftarrow{T_{PCD}}$	$T_{PCD}=\mathbf{MAC}(K_{MAC}, \widetilde{PK}_{PICC})$
$T_{PICC}=\mathbf{MAC}(K_{MAC}, \widetilde{PK}_{PCD})$	$\xrightarrow{T_{PICC}}$	

nPA Archictecture

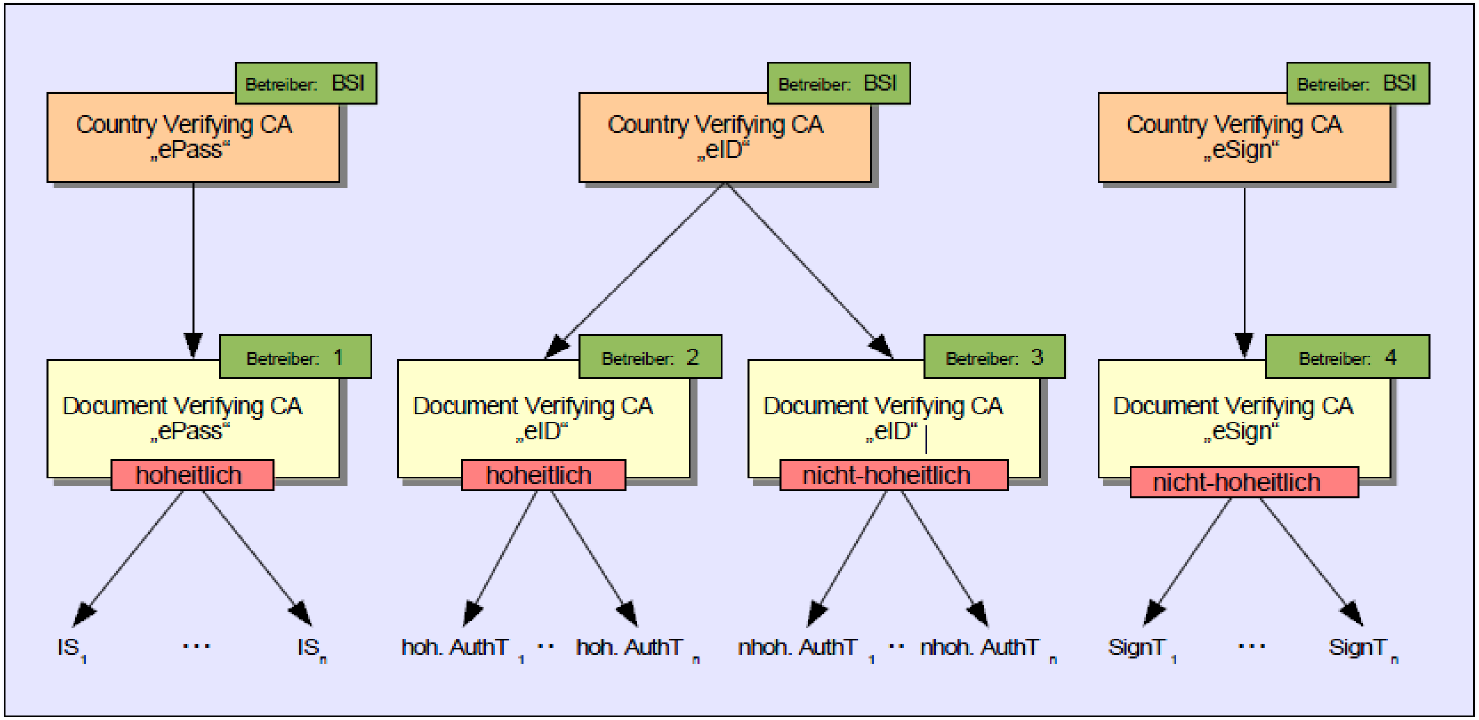
- **Komplex PKI with three independed root CAs that are operated by the german BSI.**

- **Each root ca has a subordinated issueing ca, which is called the "Document Verifying" CA (DVCA).**

- **DVCAs for ePass- and eID-fuctionality issue cv certificates. DVCA for eSing-Application issues X.509 certificates.**

nPA – Supporting Background Infrastructure

- **EAC PKIs [TR-03128], p.19**



Country Verifying CA „ePass“ (Betreiber: BSI)

Country Verifying CA „eID“ (Betreiber: BSI)

Country Verifying CA „eSign“ (Betreiber: BSI)

Document Verifying CA „ePass“ (Betreiber: 1), hoheitlich

Document Verifying CA „eID“ (Betreiber: 2), hoheitlich

Document Verifying CA „eID“ (Betreiber: 3), nicht-hoheitlich

Document Verifying CA „eSign“ (Betreiber: 4), nicht-hoheitlich

IS_1 … IS_n
hoh. $AuthT_1$ ·· hoh. $AuthT_n$
nhoh. $AuthT_1$ ·· nhoh. $AuthT_n$
$SignT_1$ … $SignT_n$

Legende

CA	= Certification Authority	**IS**	= Inspektionssystem
ePass	= ePass-Anwendung	**hoh.**	= hoheitliches
eID	= elektronischer Identitätsnachweis (Anwendung)	**nhoh.**	= nicht-hoheitliches
eSign	= elektronische Signatur (Anwendung)	**AuthT**	= Authentisierungsterminal
		SignT	= Signaturterminal

Enterprise Integration of the NPA

Enterprise Integration of the nPA

- **Szenarios**
- **Qrganizational Requirements**
- **Technical Requirements**
- **Risks**
- **Recommendations**

+

Enterprise Integration of the nPA

- **Assumption /Pre-Condition**
  - You want to do smartcard logon

- **Enterprise-Focus**
  - Active Directory

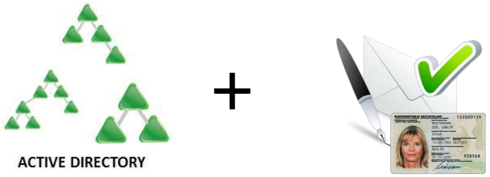
⇒Smartcard (= nPA) logon to Active Directory

  - Out of scope: SSO to other resources

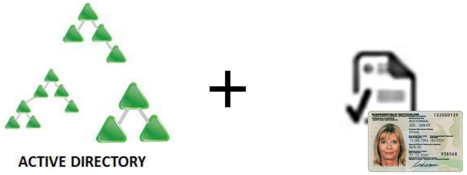
Three Szenarios

- **Smartcard logon with nPA and QES**

- **Smartcard logon with nPA and eID**



- **Smartcard logon with nPA and additional certificate (on nPA)**



Common Requierements

- **Organizational Requirements**
  - "Competence Team" for smartcard logon with nPA
    - May be part of the "Active Directory-Team"
  - Interface to the data protection officer (DSB) required
  - Interface to the german BSI (recommended) or eID-service provider (required if eID-service is used)

Common Requierements

- **Technical Requirements User PC**
  - Smartcard (nPA)
    - eID function activation required
  - Card reader
    - Compatible with nPA
  - Card reader driver
    - Available for Windows, Linux, Mac OS X, Terminal Servers (Windows, Citrix)
  - Middleware (AusweisApp)
    - Available *but not* linked to the Microsoft GINA /Credential Provider

Common Requierements

- **Technical Requirements Active Directory**
  - Depend of the scenario

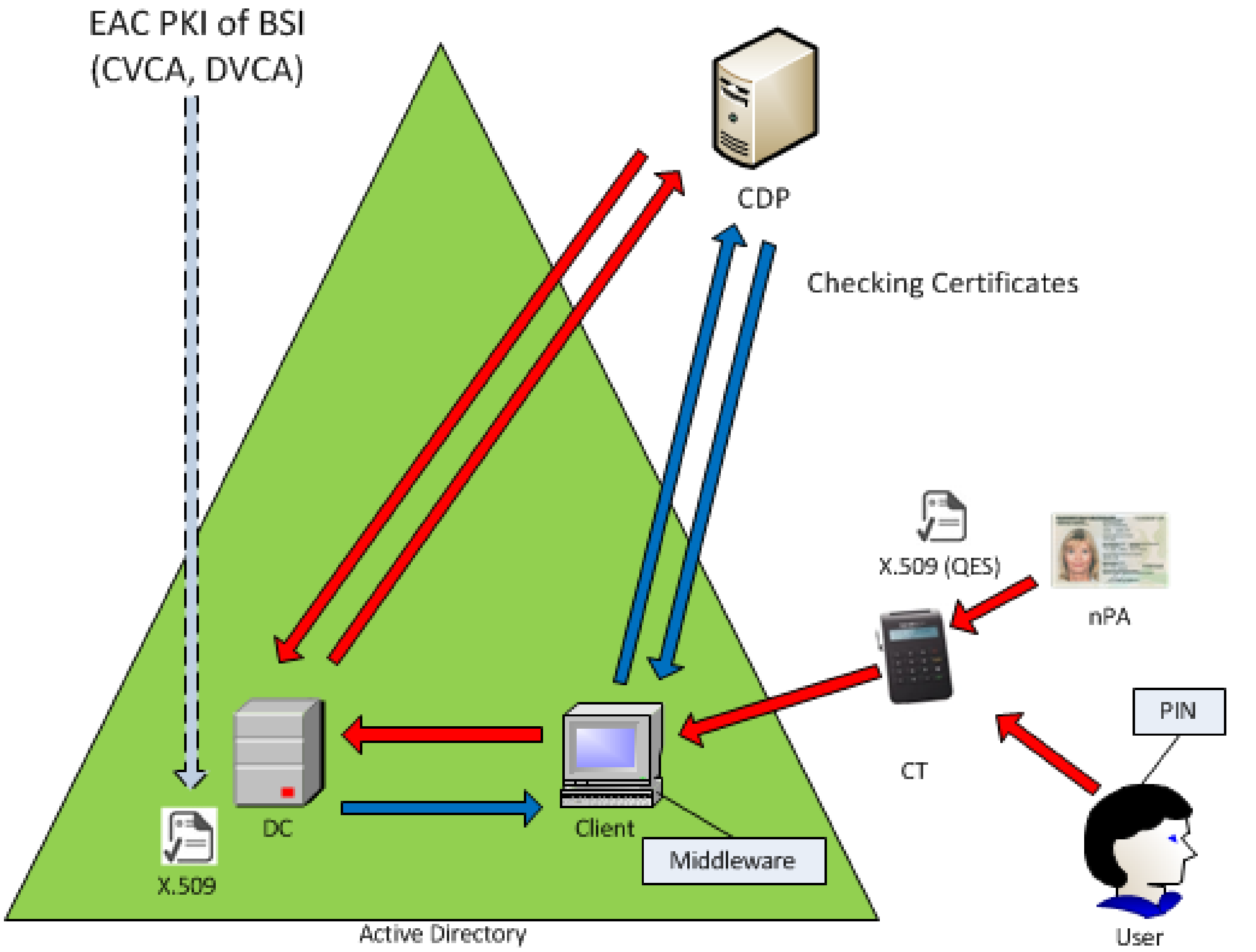
- **Technical Requirements Infrastructur**
  - CRL download required

Smartcard login with nPA and QES

- **Implementation steps**
  - Enable the nPA to talk with the computer
    - Ok
  - Download the QES certificate
    - Ok

  - Enable the computer to use QES certificate for domain login
    - ! Caveat 1: Middleware currently not integrated in computer login
    - ! Caveat 2: QES certificate currently not suitable (does not contain suitable ECDH key)
  - Enable Active Directory to accept user certificates of a not integrated CA
    - Ok (one command per CA)

Smartcard login with nPA and QES

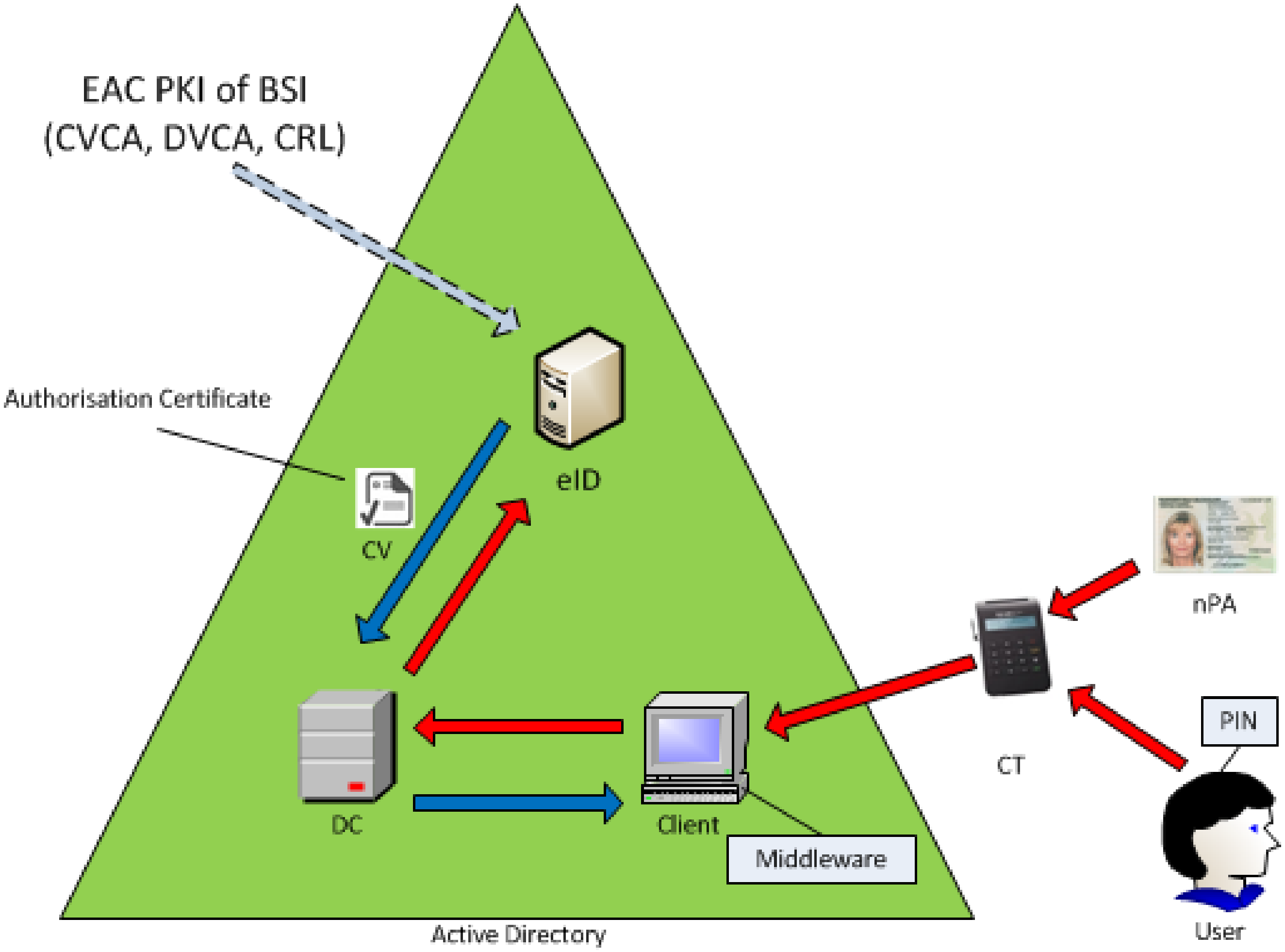


Smartcard login with nPA and eID

- **Implementation steps**
  - Enable the nPA to talk with the computer
    - Ok

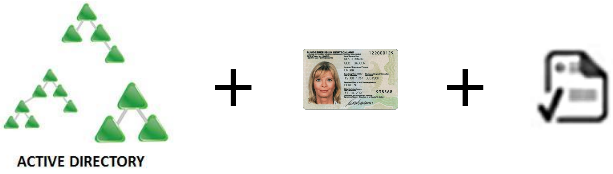
  - Caveat: Implement eID service in Active Directory
    - Via service provider or via own eID server
    - ! Caveat: Adaption of Active Directory logon process required
    - ! Caveat: Middleware currently not integrated in computer login

Smartcard login with nPA and eID



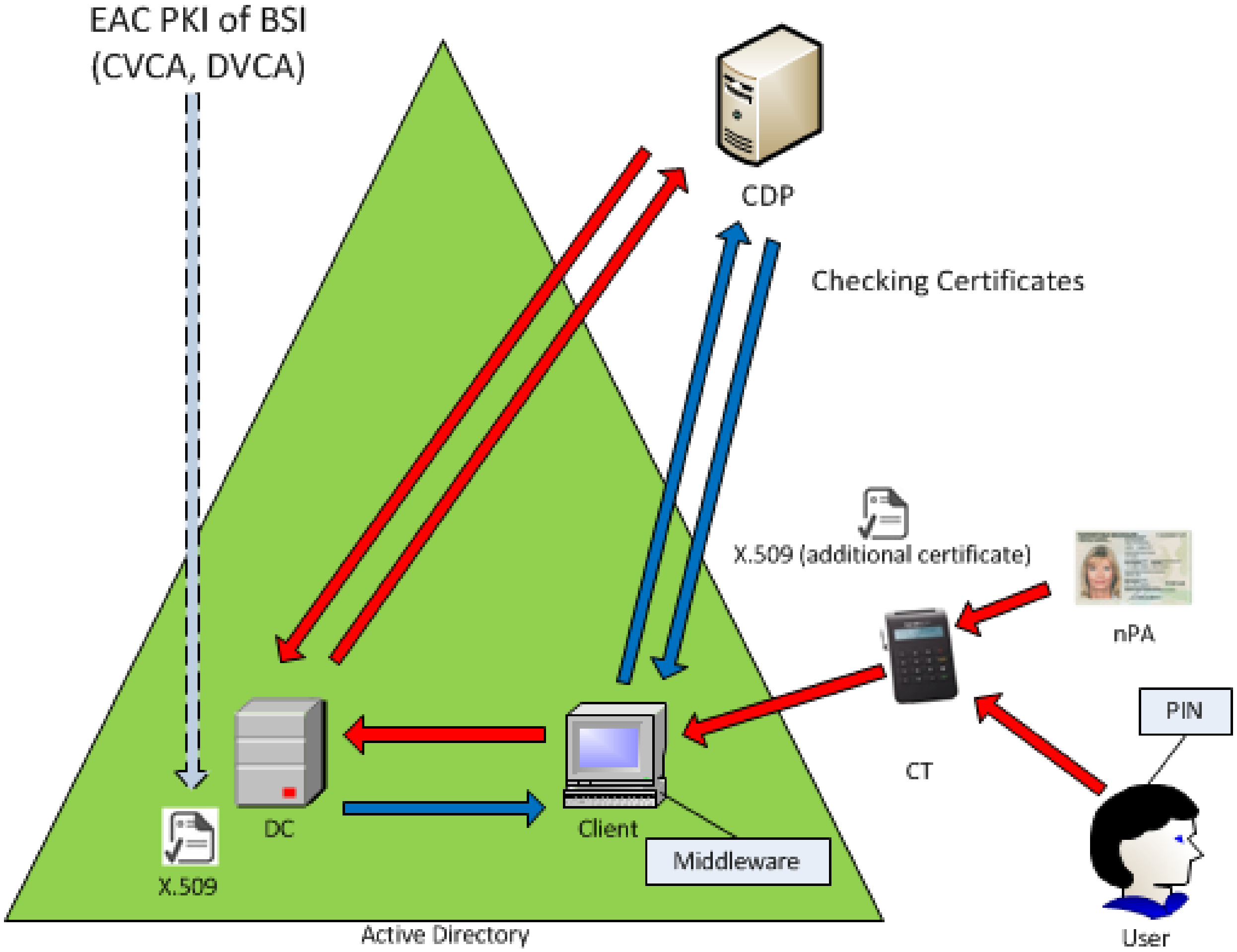
Smartcard logon with nPA and additional certificate (on nPA)

- **Implementation steps**
  - Enable the nPA to talk with the computer
    - Ok



  - Download additional certificate on nPA
    - !! Caveat 1: Use of additional certificate currently not supported by eSign application on nPA
    - ! Caveat 2: Currently only download of *one* QES certificate supported
  - Enable the computer to use the additional certificate for domain login
    - ! Caveat 1: Middleware currently not integrated in computer login
  - Enable Active Directory to accept user certificates of a not integrated CA
    - Ok (one command per CA)

Smartcard logon with nPA and additional certificate (on nPA)



Threats

- **Compromise of governmental PKI (means):**
  - Compromise of root ca or issueing ca
    - not very probable
  - Compromise of nPA chip (EAL4+ certified)
    - not very probable
  - Compromise of PACE
    - not very probable

- **Compromise of middleware (AusweisApp)**
    - not relevant in the szenario smartcard logon with nPA and QES

Threats

- **Compromise of eID server /service**
  - not very probable, but will depend on implementation

- **Compromise of user PC**
  - not relevant in the szenario smartcard logon with nPA and QES
- **User /data protection officer vetoes use of nPA for user logon**
- **Unexperienced user blocks QES- /eID functionality**

Vulnerabilities

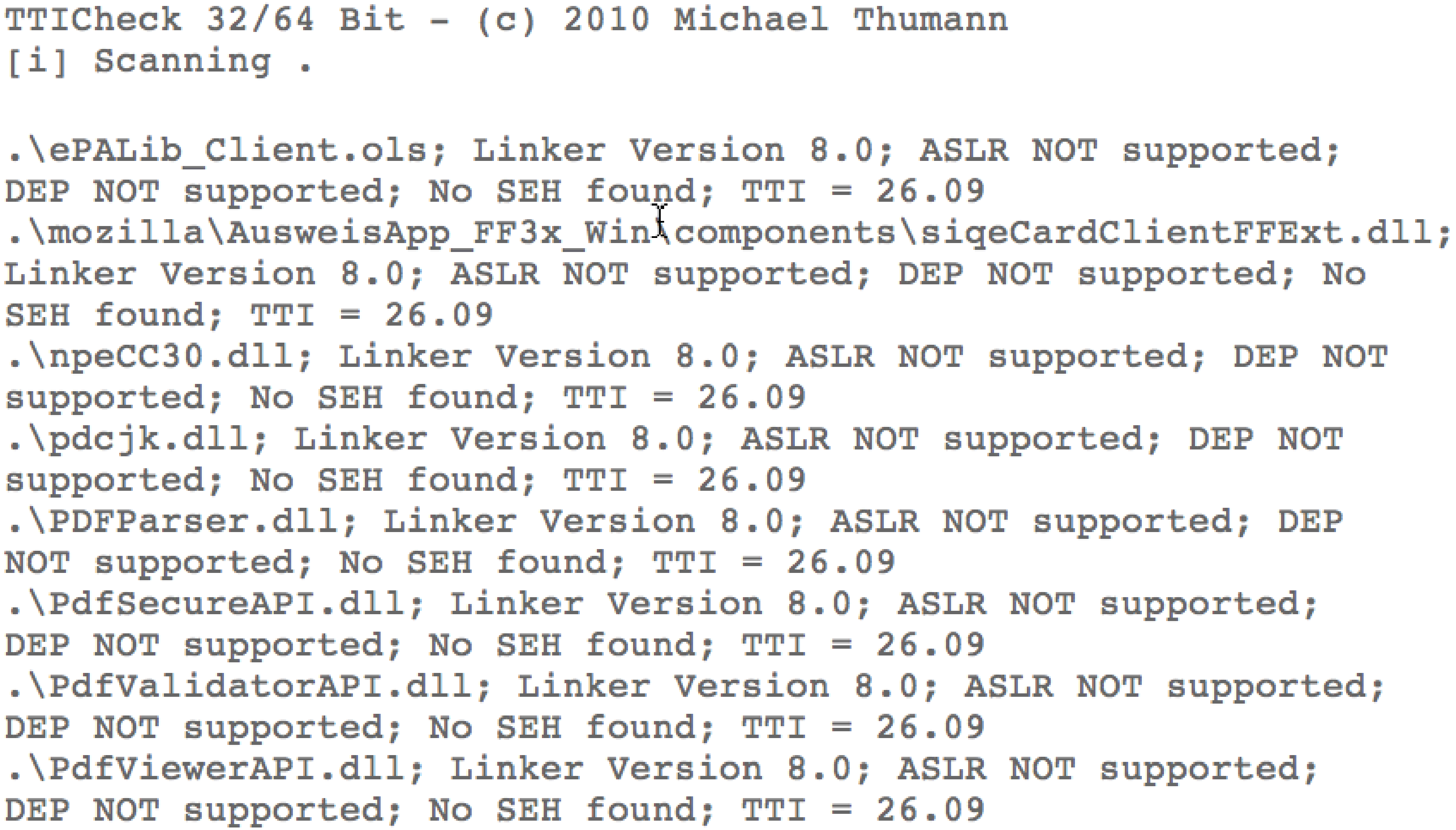
- **Middleware /AusweisApp not prepared for centralized management**
  - Updates?
  - Configuration?

- **AusweisApp had vulnerabilities in the past**
- **Only available for germans**
  - Electronic residence title (with same technical funcionality) will be available for people who live in germany

ERNW´s security research on AusweisApp

- **Because of a disclosed security vulnerability related to the update mechanism, we started some quick research for ourselves.**
- **First we checked the binaries with our TTI metric to check, if the AusweisApp was build with security in mind.**
- **Second step was to decompile the AusweisApp and look at the code itself.**
- **We were using parts of our code review approach**
- **So let‘s answer these questions ☺**

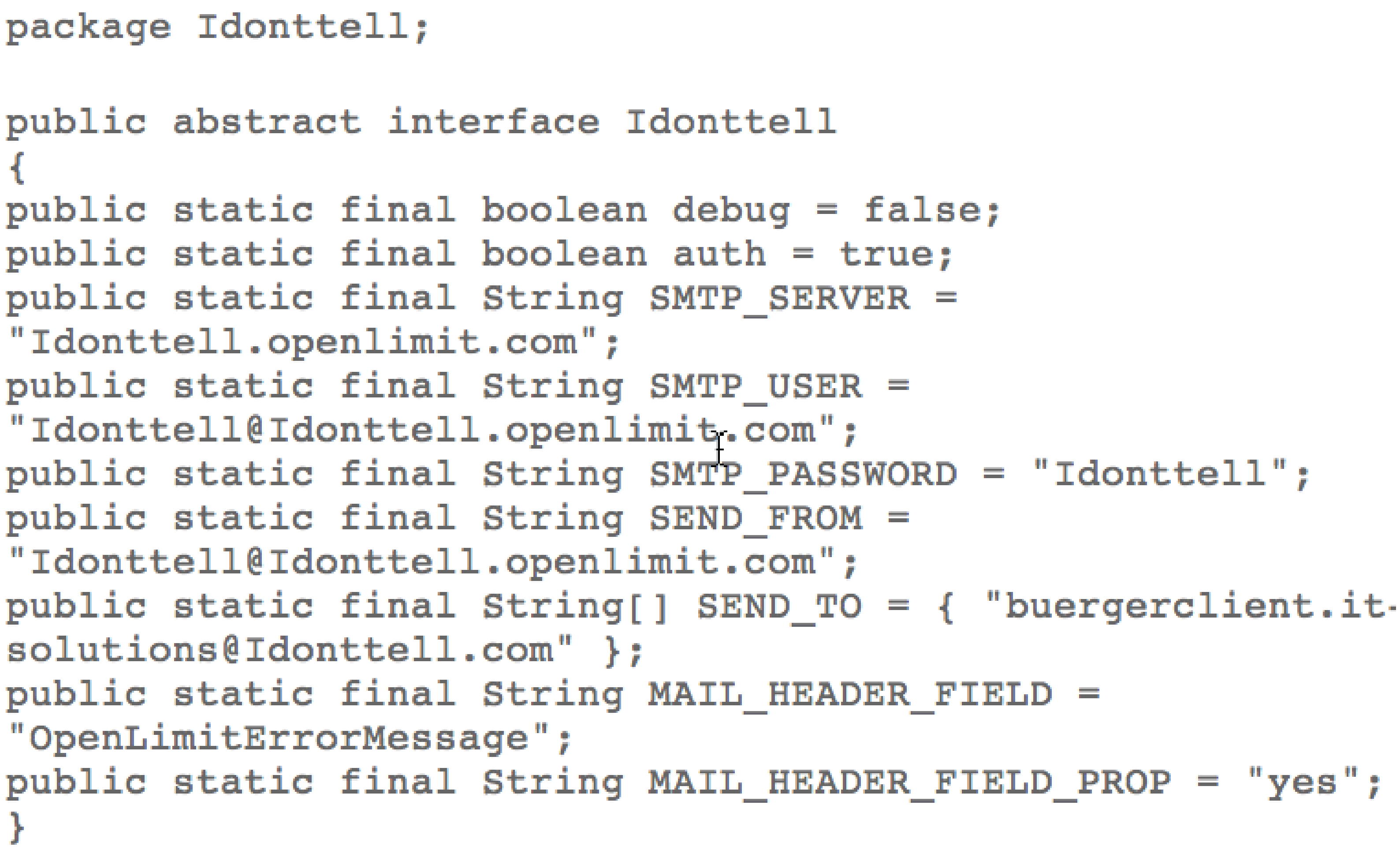
ERNW´s security research on AusweisApp: TTI



```
TTICheck 32/64 Bit - (c) 2010 Michael Thumann
[i] Scanning .

.\ePALib_Client.ols; Linker Version 8.0; ASLR NOT supported;
DEP NOT supported; No SEH found; TTI = 26.09
.\mozilla\AusweisApp_FF3x_Win\components\siqeCardClientFFExt.dll;
Linker Version 8.0; ASLR NOT supported; DEP NOT supported; No
SEH found; TTI = 26.09
.\npeCC30.dll; Linker Version 8.0; ASLR NOT supported; DEP NOT
supported; No SEH found; TTI = 26.09
.\pdcjk.dll; Linker Version 8.0; ASLR NOT supported; DEP NOT
supported; No SEH found; TTI = 26.09
.\PDFParser.dll; Linker Version 8.0; ASLR NOT supported; DEP
NOT supported; No SEH found; TTI = 26.09
.\PdfSecureAPI.dll; Linker Version 8.0; ASLR NOT supported;
DEP NOT supported; No SEH found; TTI = 26.09
.\PdfValidatorAPI.dll; Linker Version 8.0; ASLR NOT supported;
DEP NOT supported; No SEH found; TTI = 26.09
.\PdfViewerAPI.dll; Linker Version 8.0; ASLR NOT supported;
DEP NOT supported; No SEH found; TTI = 26.09
```

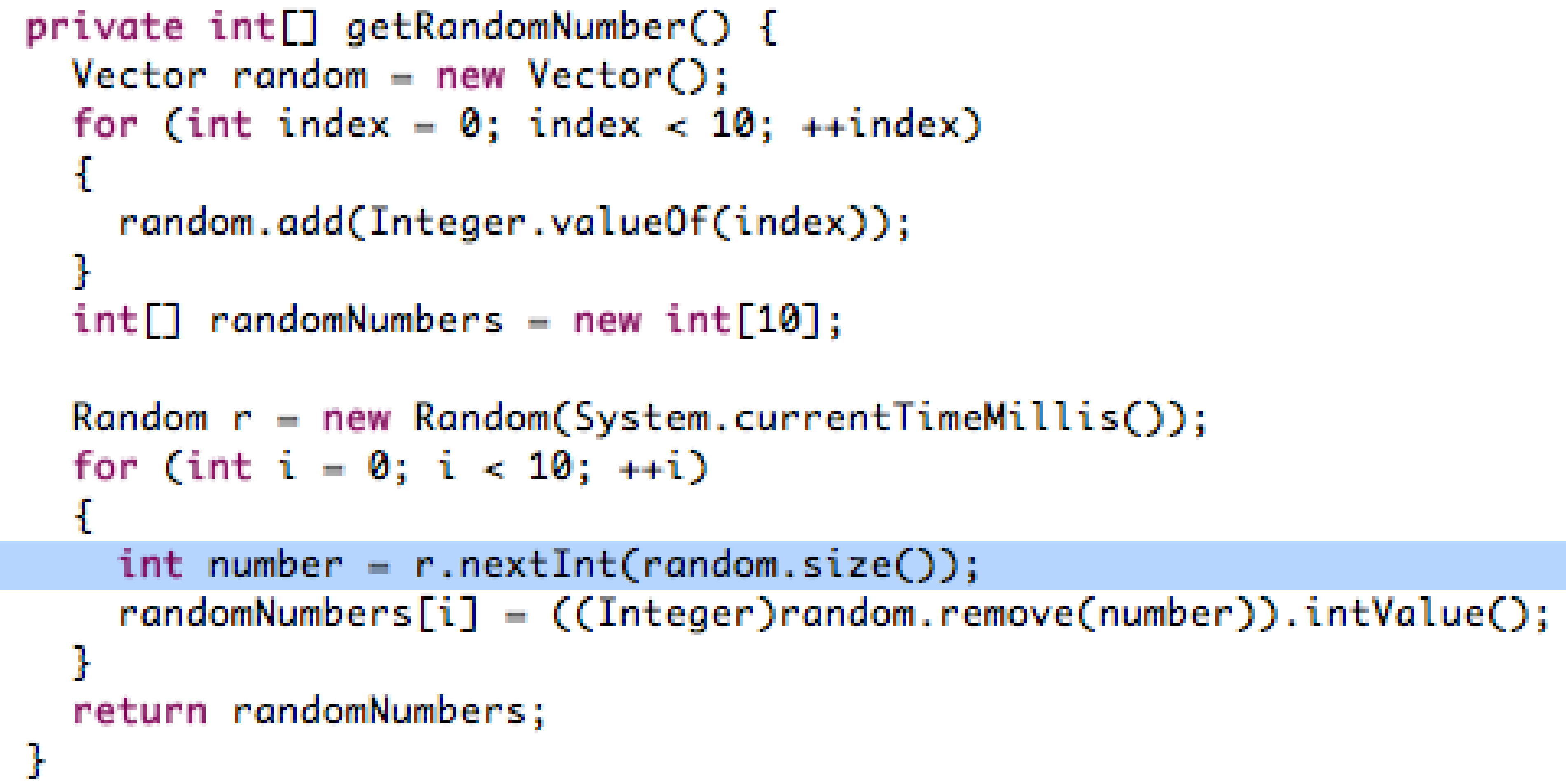
ERNW´s security research on AusweisApp: Passwords, ouch!



```
package Idonttell;

public abstract interface Idonttell
{
public static final boolean debug = false;
public static final boolean auth = true;
public static final String SMTP_SERVER =
"Idonttell.openlimit.com";
public static final String SMTP_USER =
"Idonttell@Idonttell.openlimit.com";
public static final String SMTP_PASSWORD = "Idonttell";
public static final String SEND_FROM =
"Idonttell@Idonttell.openlimit.com";
public static final String[] SEND_TO = { "buergerclient.it-
solutions@Idonttell.com" };
public static final String MAIL_HEADER_FIELD =
"OpenLimitErrorMessage";
public static final String MAIL_HEADER_FIELD_PROP = "yes";
}
```

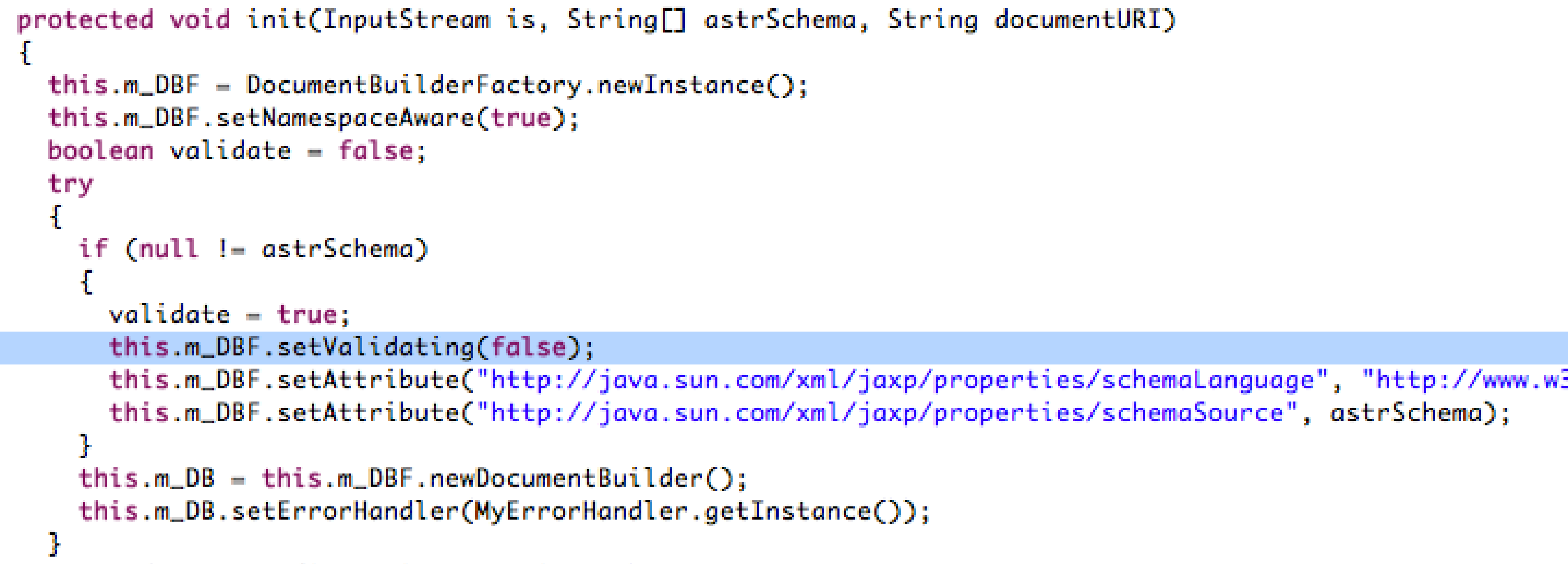
ERNW´s security research on AusweisApp: Weak crypto???



```
private int[] getRandomNumber() {
  Vector random = new Vector();
  for (int index = 0; index < 10; ++index)
  {
    random.add(Integer.valueOf(index));
  }
  int[] randomNumbers = new int[10];

  Random r = new Random(System.currentTimeMillis());
  for (int i = 0; i < 10; ++i)
  {
    int number = r.nextInt(random.size());
    randomNumbers[i] = ((Integer)random.remove(number)).intValue();
  }
  return randomNumbers;
}
```

ERNW´s security research on AusweisApp: No XML validation



```
protected void init(InputStream is, String[] astrSchema, String documentURI)
{
  this.m_DBF = DocumentBuilderFactory.newInstance();
  this.m_DBF.setNamespaceAware(true);
  boolean validate = false;
  try
  {
    if (null != astrSchema)
    {
      validate = true;
      this.m_DBF.setValidating(false);
      this.m_DBF.setAttribute("http://java.sun.com/xml/jaxp/properties/schemaLanguage", "http://www.w3
      this.m_DBF.setAttribute("http://java.sun.com/xml/jaxp/properties/schemaSource", astrSchema);
    }
    this.m_DB = this.m_DBF.newDocumentBuilder();
    this.m_DB.setErrorHandler(MyErrorHandler.getInstance());
  }
```

Combined cost-risk-control view

Scenario			
	Cost Factors	**Main Risks**	**Controls**
nPA + QES for AD logon	Integration of middleware in user logon; Domain controller certificates from official PKI; Certificate design requires additional ECDH key for ECDSA certificate.	Lost or stolen nPA; vetoed use of nPA for user logon; compromise of a governmental PKI component.	Defined processes for replacement of nPA; alternativ logon should be defined; users and data protection officer must be consulted before the decision to implement nPA for user logon.
nPA + eID for AD logon	Integration of middleware in user logon; integration of eID server or service in Active Directory; cost of eID server or service.	Lost or stolen nPA; vetoed use of nPA for user logon; compromised AusweisApp; compromise of a governmental PKI component.	Defined processes for replacement of nPA; alternativ logon should be defined; defined processes for compromised AusweisApp; alternativ middleware; users and data protection officer must be consulted before the decision to implement nPA for user logon.
nPA + additional certificate for AD logon	Yet not possible to define.	Scenario might not be possible.	To be defined.

Recommendations

- **Speak soon with users, worker´s council and the data protection officer if you plan using nPA for user logon.**
- **Presently, Active Directory integration of the nPA is not possible; observe the evolution of nPA enterprise integration**
  - especially the evolution of eID services
- **Plan for replacement scenarios of nPA with alternative user credentials in case of, lost, blocked or compromised nPA.**

Recommendations

- Use only certified card readers, at least a standard card reader (not basic!)
- Use only certified middle ware.
- If you do not plan to use the nPA + QES certificate for user logon, use at least a standard reader with display.

Summary

- **nPA enterprise integration for Active Directory logon is currently not possible but might be possible within 6 – 12 months.**

- **nPA enterprise integration for Active Directory logon is seductive, because**
  - Complete PKI is run by the german government.
  - PKI of german government promises to be highly reliable in terms of C, I, A.
  - CC EAL4+ confirmation of nPA
  - Cost for smartcard logon with nPA will be far beyond cost of an own PKI with smartcard logon (not nPA).

Summary

- **User might not be willing to use nPA for enterprise user logon; so speak soon with users, worker´s council and the data protection officer.**

References

- [Sec_Ana_EAC] Dagdelen, Özgür u. Fischlin, Marc**:** Security Analysis of the Extended Access Control Protocol for Machine Readable Travel Dokuments.
- [TR-03111] BSI: Elliptic Curve Cryptography, v.1.11
- [TR-03116-2] BSI: eCard-Projekte der Bundesregierung. Stand 2010 Revision.
- [DK] Dennis Kügler: Extended Access Control: Infrastructure and Protocol, Berlin 2006.

Questions & Answers

- **Stay tuned with us ;-)**