Trusted digital Identity
aka
electronic signature
(NOT digital signature)

Christopher David Wolf
Forest Information Technology
FH-Eberswalde
03.05.2007

What is a Trusted digital Identity?

Identity: „the distinguishing character or personality of an individual“

Digital: „of, relating to, or being data in the form of especially binary digits“ (electronic)

Trust: „assured reliance on the character, ability, strength, or truth of someone or something“

Identification: „evidence of identity“

(merriam-webster dict.)

An electronic signature (SigG)

is the

LEGAL EQUIVALENT

of your physical signature!

An electronic signature (SigG)

is the

LEGAL EQUIVALENT

of your physical passport!

Legal basis in Germany (EU) (SigG)

Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) vom 16. Mai 2001 (BGBl. I S. 876) zuletzt geändert durch Art. 1 des Ersten Gesetzes zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04. Januar 2005 (BGBl. I S. 2)
(Reevaluated fromt the first EU law pertaining to e. signatures in 1997)

Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) vom 16. November 2001 (zuletzt geändert durch Artikel 2 des 1. Gesetzes zur Änderung des Signaturgesetzes vom 04. Januar 2005

(DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures)

Electronic- vs. Digital signature

electronic signature: "an electronic sound, symbol, or process, attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." (Uniform Electronic Transaction Act or "UETA" released by NCCUSL in 1999)

digital signature:a type of asymmetric crytography used to simulate the security properties of a signature in digital, rather than written, form

A digital signature is a subset of an electronic signature.

(Wikipedia)

Structures of responsibility in Germany

Bundesministerium der Justiz

Makes and reformes the underlying law (SigG) as well as the underlying edict (SigV)

Bundesnetzagentur

Operates the national root-CA for Germany, accredits other certificate providers, publishes validation authorities, Algorithms, Products, public key of the root-CA, and certificate providers

Bundesamt für Sicherheit in der Informationstechnik

Researches and suggests possible algorithms

TÜViT® +1

Tests products, solutions and security environments upon their conformity to the given laws and edicts

D-TRUST WE DEFINE SECURITY +

The CA (certificate authority), issues certificates to users. Acts as the digital equivalent to a passport issuing ministry.

Key necessities of an electronic signature

Integrity: being able to prove, that an electronic document is in an unaltered state. i.e. the document that is RECEIVED is the same document that was SENT.

Identity: being able to identify the SENDER (beyond a reasonable doubt)

Verification: both **Integrity** and **Identity** must be provable over a *long (decades)* period of time.

An electronic signature DOES NOT ensure the CONFIDENTIALITY of a document! (optional functionality, which has to be incorporated seperatly!)

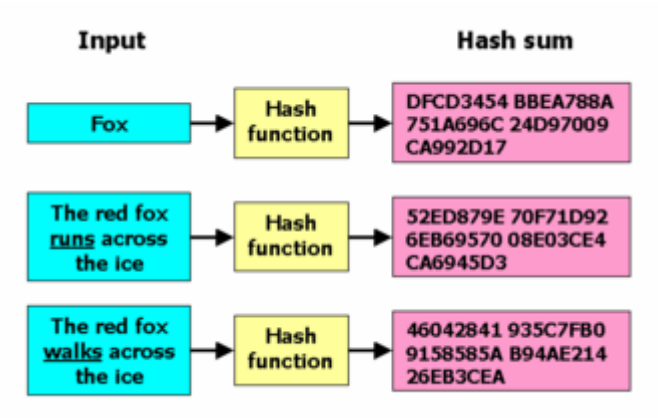
What can I do with it?

What can‘t you do when presenting your passport and giving your signature?

The INTEGRITY of a document is secured by two steps:

1. Calculate an electronic fingerprint from a digital document;

   -> HASH FUNCTION



(Wikipedia)

Most crucial demands on a hash function:

a. Calculating the fingerprint of an identical document must yield the same result every time.

b. Different documents must in all probability have different fingerprints.

2. The HASH fingerprint is attached to the electronic document.

➢INTEGRITY	IDENTITY	VERIFICATION

➢testing

Checking if a document has been altered:

1. Seperate the original fingerprint from the document.
2. Calculate the fingerprint of the document on your own computer, thereby receiving a reference fingerprint.

If the original and the reference fingerprint are the same, then the document was not tampered with.

Sound INTEGRITY

If the document was tampered with, then the fingerprints of the original and the reference fingerprint will not be the same.

Unsound INTEGRITY

INTEGRITY	IDENTITY	VERIFICATION

➢Electronic signature

A fingerprint is unpersonal, i.e.

- Identical Documents will have the same fingerprint (depending on the HASH function used!), and do not vary from person to person.

Personalizing a fingerprint:

- By using a secret (privat) key of suitable lenght, RECALCULATE the HASH value (actual electronic signature); since the key can only belong to one person, the personalized fingerprint can also belong to only one person
- The secret key is called the signature key

INTEGRITY	IDENTITY	VERIFICATION

➢Certificate

To positively identify a key as belonging to a certain person without a doubt, a digital equivalent to a passport is used. This is called the certificate:

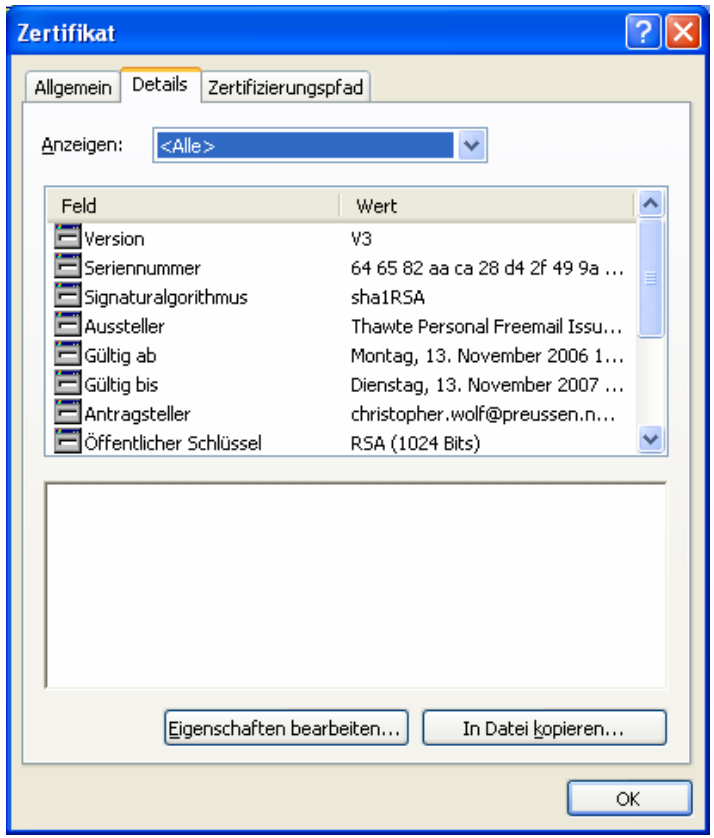
The certificate holds personal data, pertaining to the owner of the private key

It has an issued period of validity

It explicitly names the issuing authority, or *certificate authority*

The (public) signature key of the public/private key „twins“ is written out on the certificate.

To protect the certificate from manipulations, it is signed by the CA.



certmgr.msc Bundesnetzagentur

INTEGRITY	IDENTITY	VERIFICATION

➢Root CA

The issuer of a certificate is called the certificate authority.

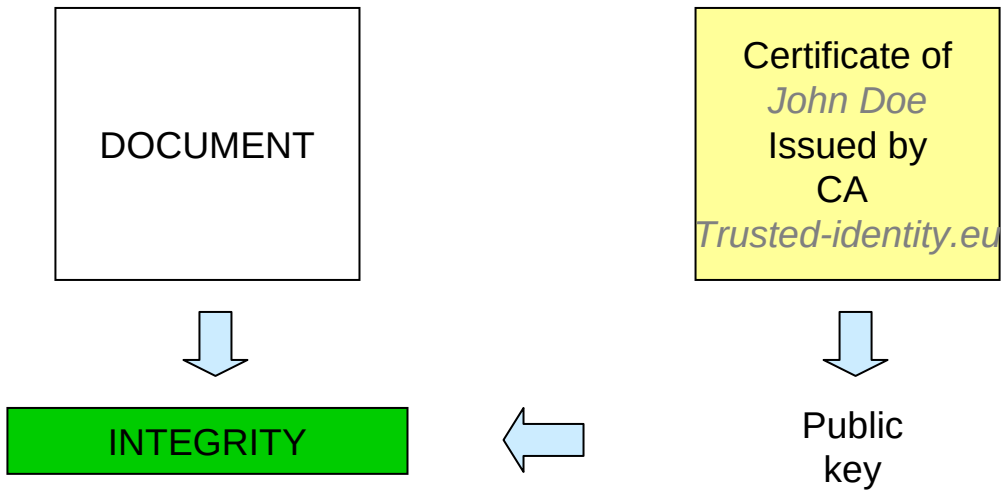
For the electronic communication, a certificate has the same functions as a passport for physical travel. It proves the identity of the keys owner/user.
Since this „proof“ needs to have a basis of trust at ist pyramidal bottom somewhere, the law regulating the these certificate authorities is very exacting and strict.
In German they are called TRUSTCENTER (engl.: certificate authorities).

The trustworthyness of a CA is build upon the security measures, that the public *believes* the institution can ensure. In the travels betweeen countries it is not necessary for every passport to look alike, it is enought to know what the passports of the neighboring countries look like and place trust in their security measures.
Since a trusted agency needs to be found (*trusted ancor / Vertrauensanker),* the Bundesnetzagentur is the final Root-CA for Germany. It issues certificates to the CAs.

INTEGRITY	IDENTITY	VERIFICATION

➢testing

Basically an electronic document is tested as such:

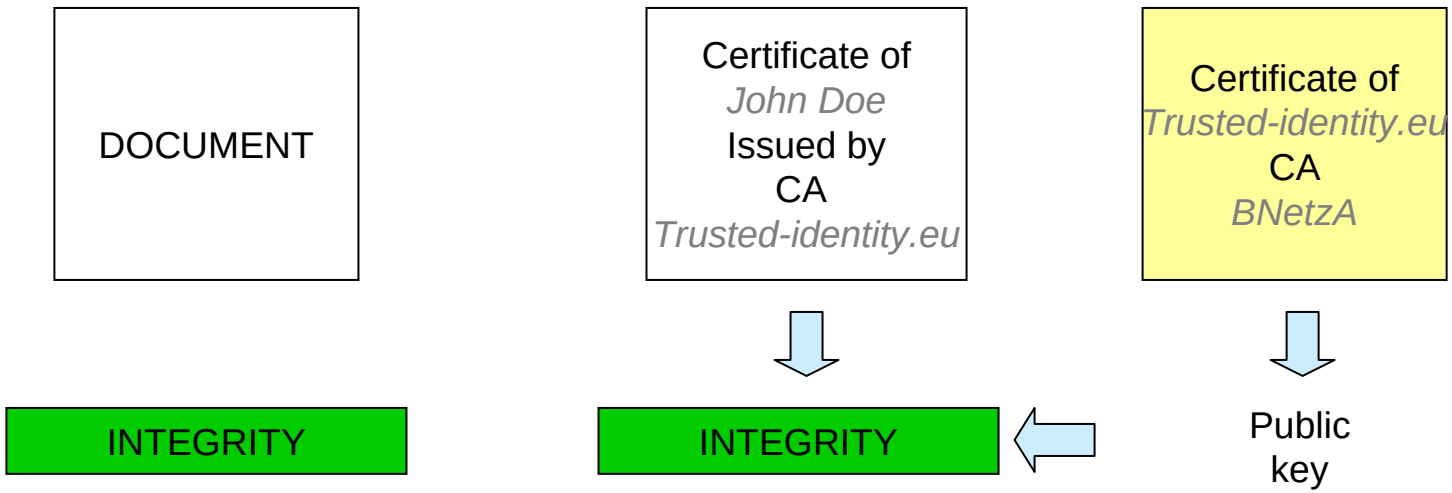


The public key is taken out of the certificate of the communication partner to test the integrity of the document.

INTEGRITY	IDENTITY	VERIFICATION

➢testing

Basically an electronic document is tested as such:

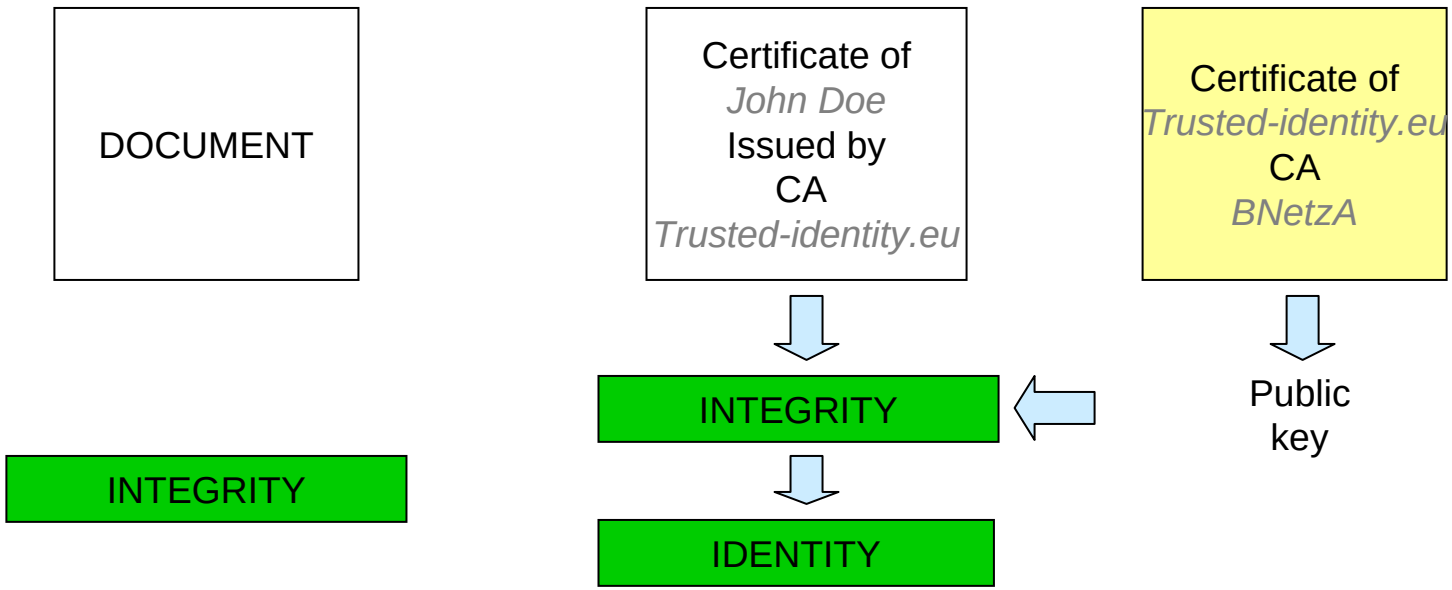


Now the public key of the CA‘s certificate is taken and used to test the integrity of your communication partners certificate.

INTEGRITY	IDENTITY	VERIFICATION

➢testing

Basically an electronic document is tested as such:

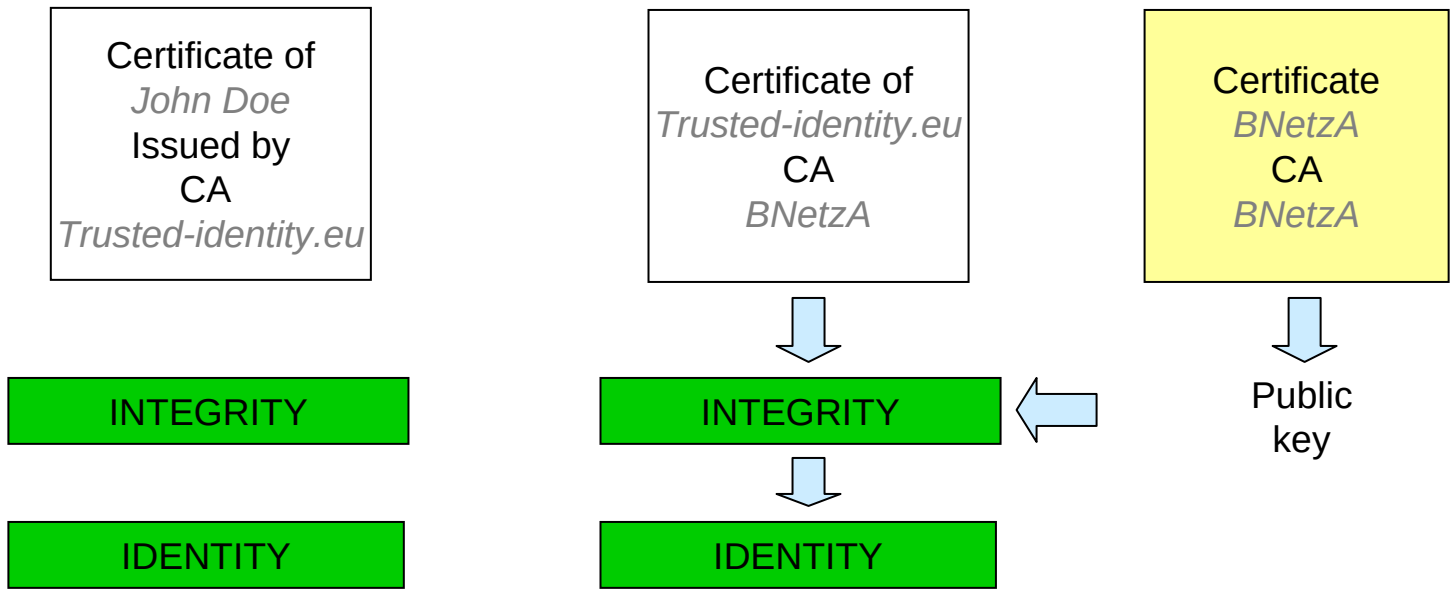


Since the public key inserted in the certificate is connected to the communication partner, his identity is proven along with the integrity of the certificate.

INTEGRITY	IDENTITY	VERIFICATION

➢testing

The trustworthyness of certificates is tested similarly.

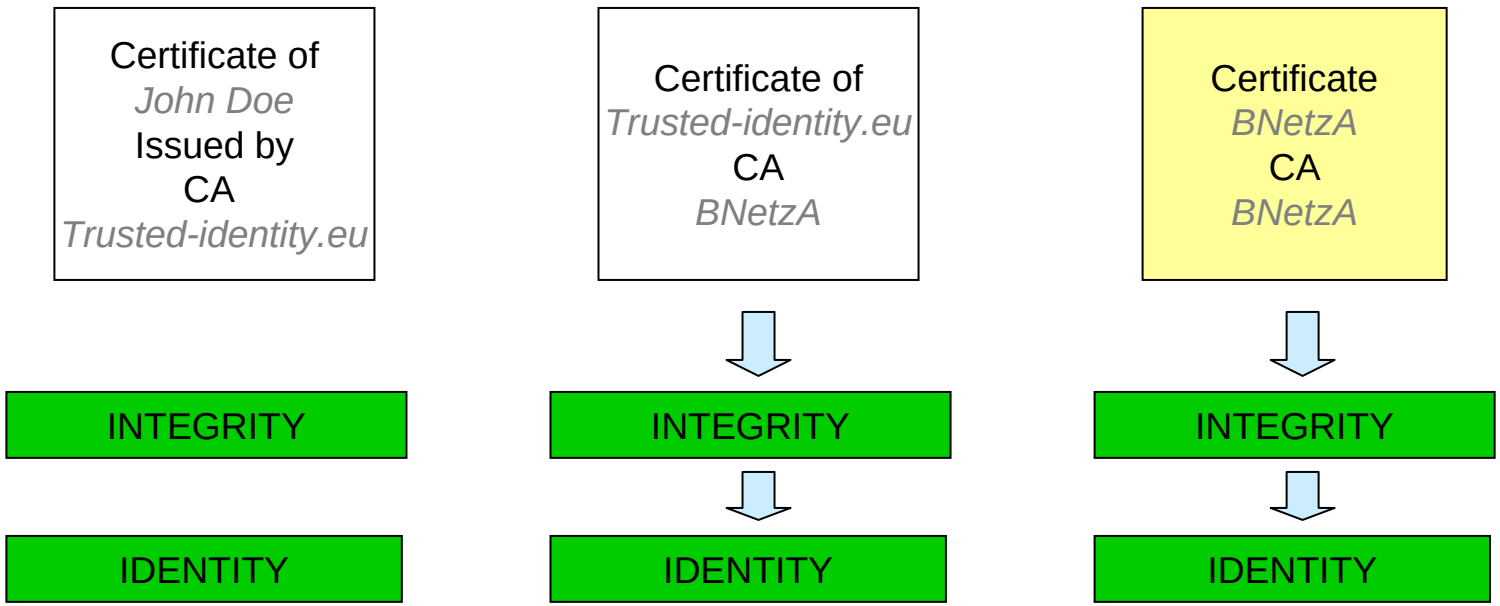


To prove the identity of the CA, the certificate of the Bundesnetzagentur is used.

INTEGRITY	IDENTITY	VERIFICATION

➢testing

The trustworthyness of certificates is tested similarly.

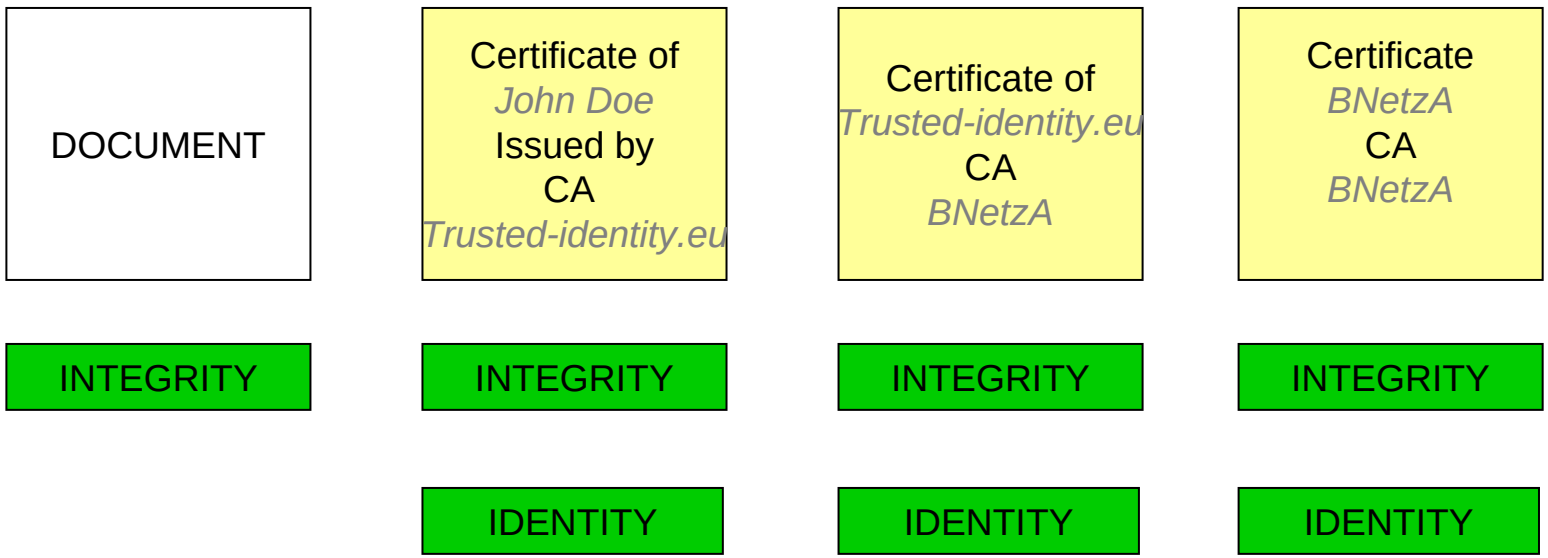


The certificate of the Bundesnetzagentur (Root-CA) can be checked directly.

INTEGRITY	IDENTITY	VERIFICATION

➢valid document

You have a validly signed document , when the integrity of the following:



has been checked. This mechanism is automated.

INTEGRITY	IDENTITY	VERIFICATION

➢DirX Trustcenter

All the necessary certificates to check if an electronically signed document is saved in lists.

Next to the list of certificates, there also exists a list of revoked certificates. This is called the Revocation List.

Certificates can be revoked, if for example the chipcard containing the private key of the user has been stolen. From the time of revocation, no valid electronic signature can be made with the private key.

The list of certificates, together with the CRL form the directory, which can be accessed 24/7 to validate or falsefy electronic signatures.

This directory, as well as the technology needed to produce new certificates are in a high security vault at the CAs location.

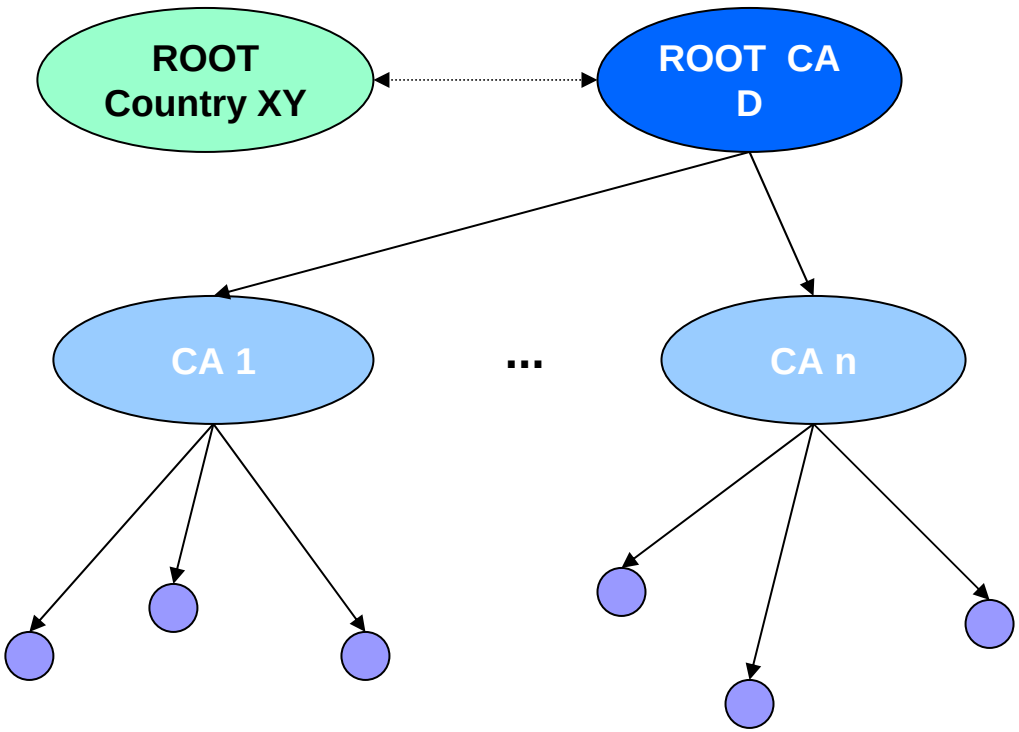
Also RAID, Cluster, Backup.

INTEGRITY	IDENTITY	VERIFICATION

➢Infrastructure

The sum of parts for the provability of electronic signatures is called the

Public Key Infrastructure.



National ROOT CA
- governmental -

Issues certificates for

Certificate Authorities
- privat -

Issues certificates for

users
Institutions, companies
privat persons

The End

Literature I

0) www.bundesnetzagentur.de/media/archive/4565.**ppt**

1) Nicht veröffentlichtes Dokument; Feinkonzept; Trustcenter der Deutschen
Rentenversicherung für Zertifizierungsdienste nach dem deutschen Signaturgesetz; Version:
01.04.03; Stand**:** 04.12.06; Pfleger: Hr. M. Pietschner, SEC GmbH

2) Nicht veröffentlichtes Dokument; Migrationskonzept; Trustcenter der Deutschen
Rentenversicherung für Zertifizierungsdienste nach dem deutschen Signaturgesetz; Version:
00.01.01; Stand**:** 19.02.07; Pfleger: Hr. D. Schmidt, SBS GmbH

3) „Digitale Signatur:Grundlagen, Funktion und Einsatz“; F. Bitzer, K. Brisch; 1999; Springer-Verlag; ISBN 3-540-65563-8

4) „Digitale Signaturen“; A. Bertsch; 2002; Springer-Verlag, (Xpert.press); ISBN 3-540-42351-6; ISSB 1439-5428; Printed in Germany

5) Elektronisches .pdf Dokument, Zugriff am 05.03.2007
Anbieter: „Anbieter im Sinne des TDG: Bundesrepublik Deutschland, vertreten durch
das Bundesministerium der Justiz, vertreten durch die Bundesministerin der
Justiz“
Titel: „Gesetz über Rahmenbedingungen für elektronische Signaturen
(Signaturgesetz – SigG)“
Aktualisiert: „Signaturgesetz vom 16. Mai 2001 (BGB1. I S. 876), zuletzt geändert durch
Artikel 3 Abs. 9 des Gesetzes vom 7. Juli 2005 (BGB1. I S. 1970; Änderung
Durch Art. 4 G v. 26.2.2007 I 179 zukünftig in Kraft)“
Adresse: http://www.gesetze-im-internet.de/bundesrecht/sigg_2001/gesamt.pdf

6) Elektronisches .html Dokument, Zugriff am 12.03.2007
Anbieter: Deutsche Rentenversicherung
Titel: „Einführung – Die Rolle des elektronischen Zertifikates im Datenaustausch“
Aktualisiert: 24.01.2007
Adresse: http://www.deutsche-rentenversicherung.de/nn_8346/SharedDocs/de/Navigation/Service/Zielgruppen/verwaltung/trustcenter/
Einf_C3_BChrung__node.html__nnn=true

7) Elektronisches .html Dokument, Zugriff am 12.03.2007
Anbieter: Deutsche Rentenversicherung
Titel: „Trustcenter“
Aktualisiert: 24.01.2007
Adresse: http://www.deutsche-rentenversicherung.de/nn_7112/SharedDocs/
de/Inhalt/Zielgruppen/04__oeffentliche__verwaltung/04__trustcenter/Einfuehrung/Trustcenter.html

Literature II

8) Elektronisches .html Dokument, Zugriff am 18.03.2007
Anbieter: D-Trust, eine Tochter der Bundesdruckerei-Group
Titel: Beantragung Ihrer D-Trust-2048-Bit-Signaturkarte
Aktualisiert: Unbekannt
Adresse: https://www.d-trust.net/internet/content/beantragung2.html
9) Elektronisches.html Dokument, Zugriff am 17.03.2007
Anbieter: Bundesnetzagentur
Titel: „FAQ“
Aktualisiert: 26.10.2006
Adresse: http://www.bundesnetzagentur.de/enid/Elektronische_Signatur/FAQ_pm.html
10) „Praxisbuch Netzwerk-Sicherheit“; J. Plötner, S. Wendzel; 2007; Galileo Press; Auflage:
2. A. ; ISBN-10: 3898428281; ISBN-13: 978-3898428286
11) Elektronisches wiki Dokument, Zugriff am 18.03.2007
Anbieter: Wikipedia
Titel: RSA-Kryptosystem
Aktualisiert: 15.03.2007
Adresse: http://de.wikipedia.org/wiki/RSA-Kryptosystem
12) Elektronisches wiki Dokument, Zugriff am 18.03.2007
Anbieter: Wikipedia
Titel: SHA1
Aktualisiert: 18.03.2007
Adresse: http://de.wikipedia.org/wiki/SHA1
13) Elektronisches wiki Dokument, Zugriff am 18.03.2007
Anbieter: Wikipedia
Titel: Bundesnetzagentur
Aktualisiert: 13.03.2007
Adresse: http://de.wikipedia.org/wiki/Bundesnetzagentur
14) Elektronisches wiki Dokument, Zugriff am 18.03.2007
Anbieter: Wikipedia
Titel: Hash-Funktion
Aktualisiert: 18.03.2007
Adresse: http://de.wikipedia.org/wiki/Hash