
LERNENDE MASCHINEN 02.05.2017
INDUSTRIE 4.0 23.05.2017
SPRACH-DIALOGE 09.05.2017
KÜNSTLICHE INTELLIGENZ
KI
BIG DATA 13.06.2017
TEAM-ROBOTIK 30.05.2017
AUTONOME SYSTEME 16.05.2017
ALTERS-ASSISTENZ
SMART SERVICE
SICHER-HEIT 20.06.2017
EMOTION & VERHALTEN

Vorlesungsreihe 2017: Künstliche Intelligenz für den Menschen: Digitalisierung mit Verstand

Mainz, 20. Juni 2017

Johannes Gutenberg Stiftungsprofessur

Datensouveränität, Privatsphärenschutz und Langzeit-Sicherheit im Zeitalter Künstlicher Intelligenz

Prof. Dr. Dr. h.c.

Johannes Buchmann

TECHNISCHE UNIVERSITÄT DARMSTADT

Technische Universität Darmstadt
Fachbereich Informatik
Hochschulstraße 10
64289 Darmstadt

Herausforderung: Langzeitsicherheit

Barack Obama
30. Januar 2015

Tonight, I'm launching a new Precision Medicine Initiative to b[illegible] d[illegible] diabetes

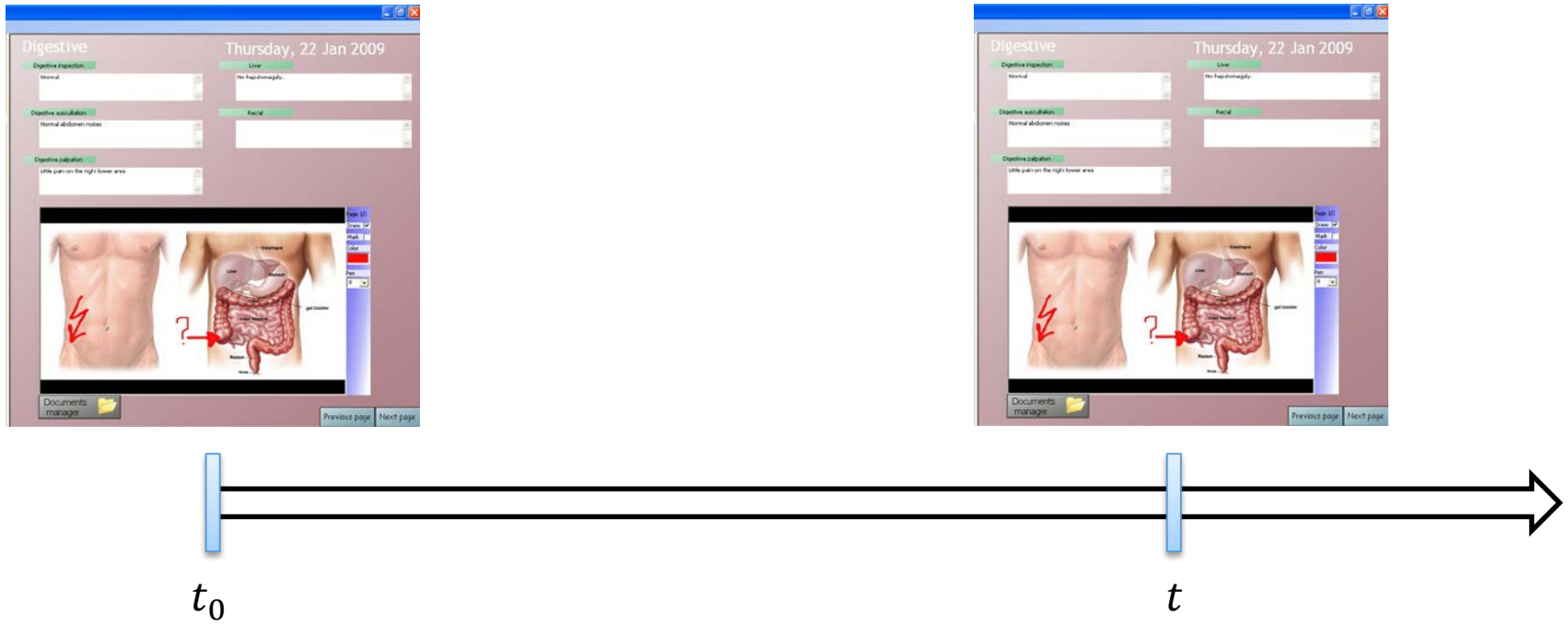
and to give all of us access to the personalized information we need to keep ourselves and our families healthier.

Erfordert Langzeit-Archivierung medizinischer Daten

Johannes Gutenberg Stiftungsprofessur

Schutzziele für langfristig archivierte Daten

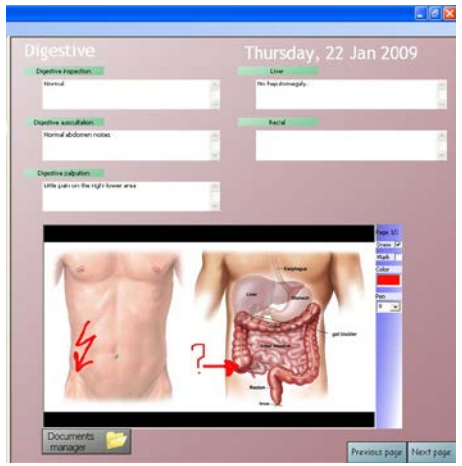
Integrität

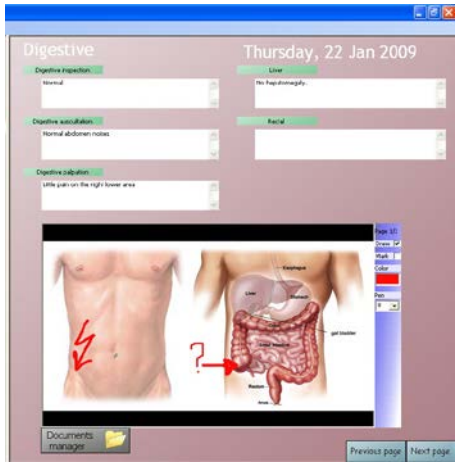


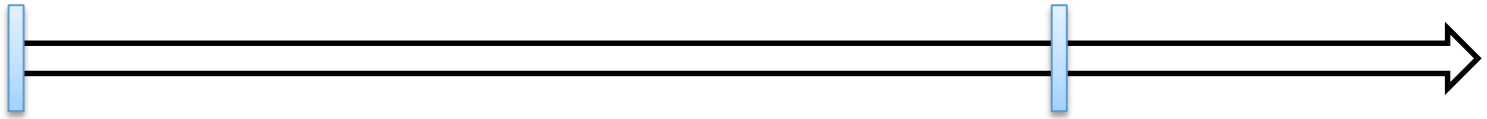
Archivierungszeitpunkt

Dokument wurde seit Zeitpunkt t_0 nicht geändert

Authentizität







t_0

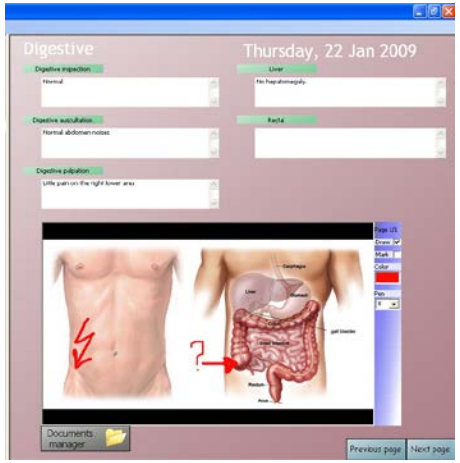
t

Archivierungszeitpunkt

Dokument wurde seit Zeitpunkt t_0 nicht geändert

und Herkunft ist verifizierbar

Vertraulichkeit

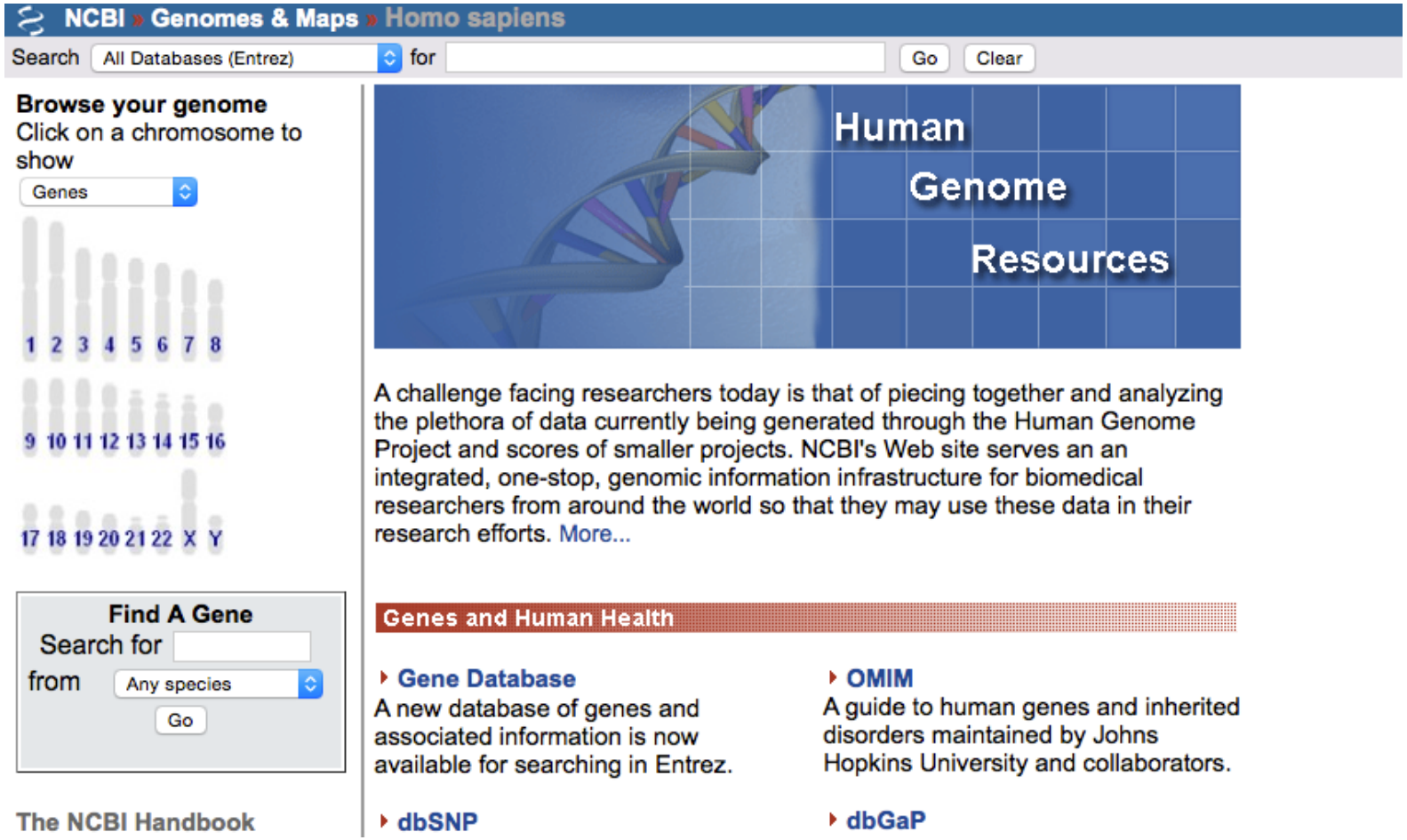


Data **in transit**

Data **at rest**

Langzeitschutz auch für:

Genomdatenbanken



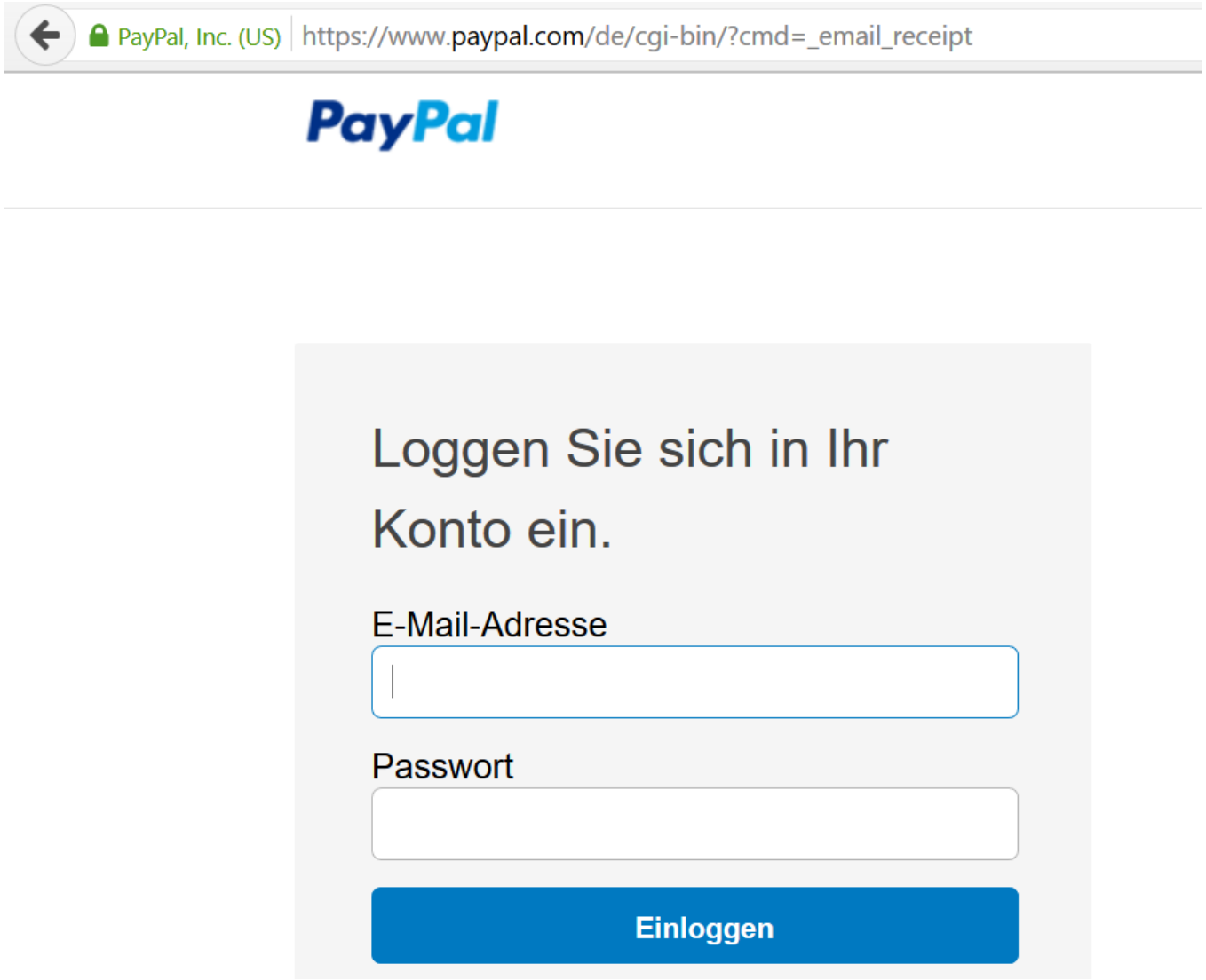
Steuerdaten

Hoheitliche Dokumente

WhatsApp

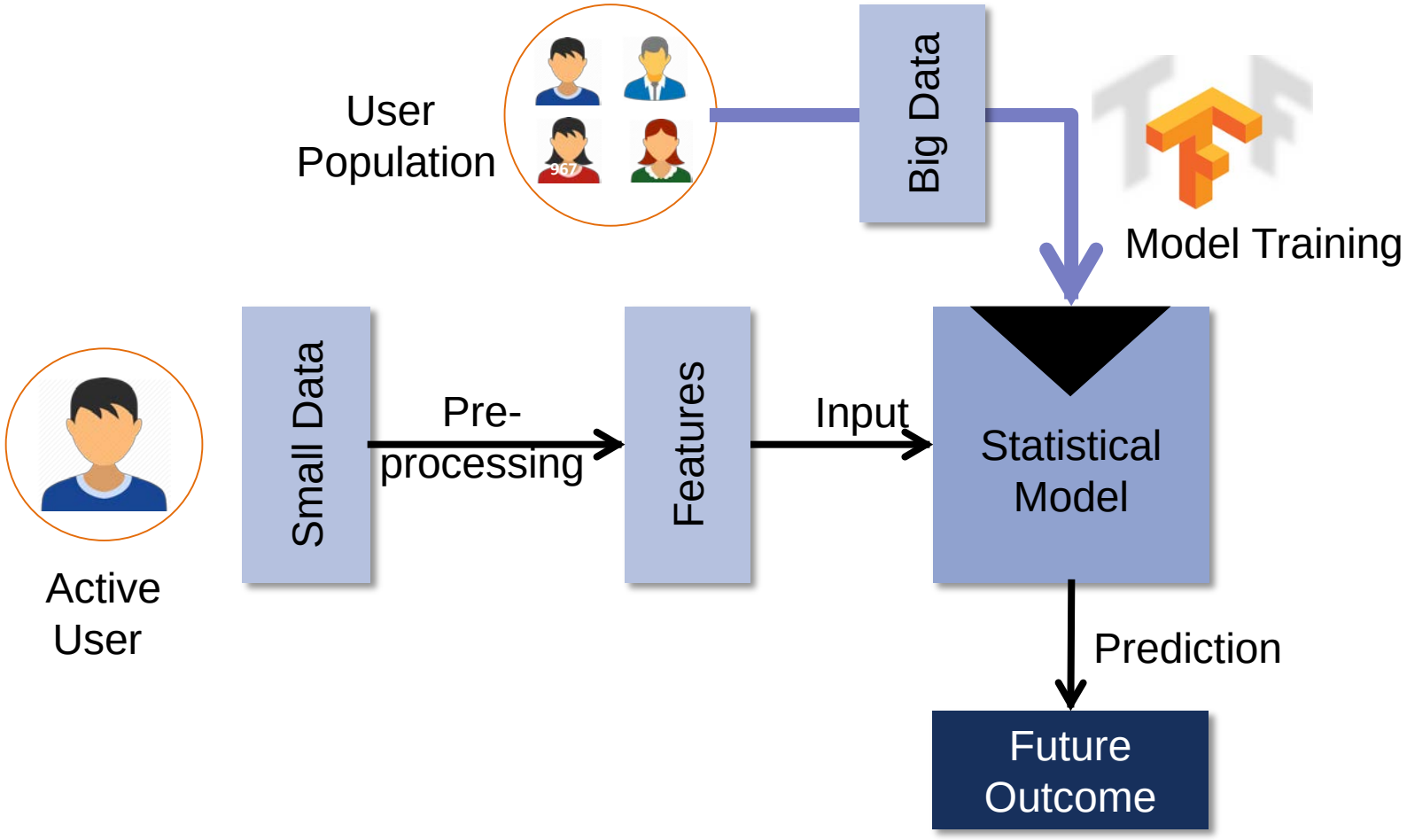
Wie lange sollen Nachrichten vertraulich bleiben?

PayPal



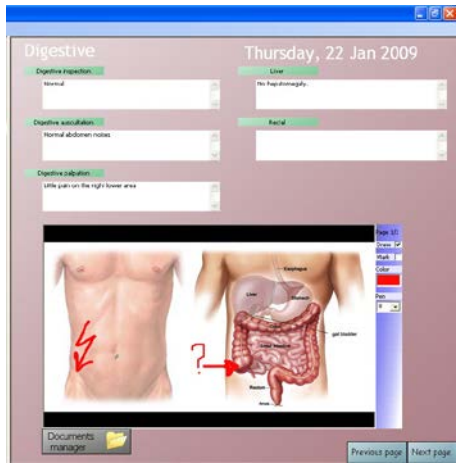
Wie lange sollen Transaktionen vertraulich bleiben?

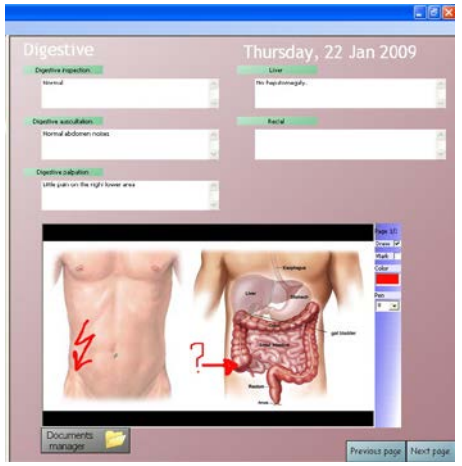
… in Anbetracht der künstlichen Intelligenz

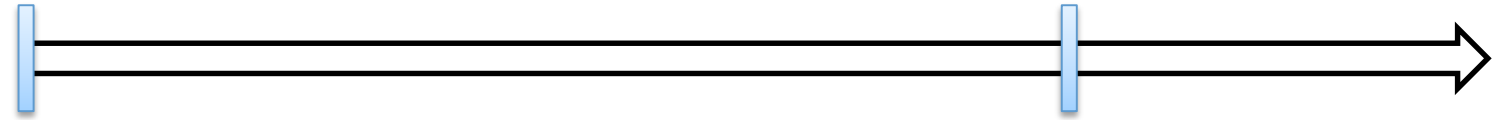


Schutz durch Kryptographie

Integrität und Authentizität







t_0 t

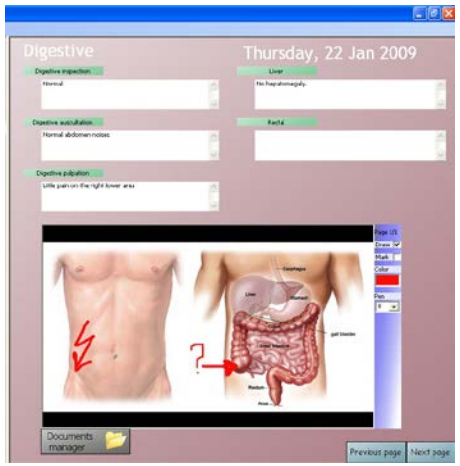
Archivierungszeitpunkt

Elektronische Signatur

Beweis: Dokument wurde seit t_0 nicht geändert und Herkunft verifizierbar

Verifikation der elektronischen Signatur

Vertraulichkeit



Data **in transit**

Verschlüsselung

Data **at rest**

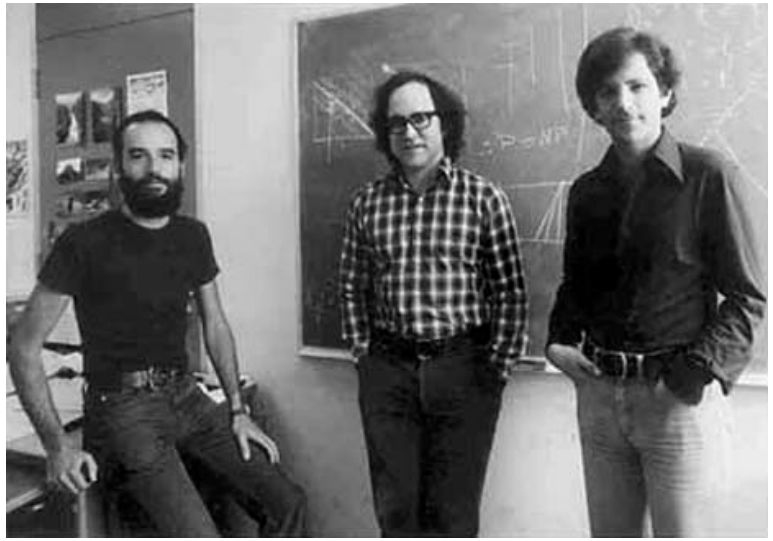
Verschlüsselung

Klassische Kryptographie kann keinen langfristigen Schutz garantieren

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman*

Pierre de Fermat
1601 - 1665



Turing Award 2002

RSA-Schlüssel

Johannes Gutenberg Stiftungsprofessur

Öffentlich: Produkt von zwei Primzahlen	Geheim: Primfaktoren
15	= 3 x 5
35	= 5 x 7
109869256229	= 123787 x 887567

Öffentlicher RSA-Schlüssel von PayPal

Johannes Gutenberg Stiftungsprofessur

31795268810366627125473790859797098391197908286525437
50773640112859051043838263250796844647566647073676507
37698350040734989120408350361119844369827869651498796
73665411793622083038631384645332380078749777062290203
70398442691648609936395220964249973923183224282326242
93883124379061631765073423204610042801378799675461282
34413259882008909669991881742777224061960485068828406
51732990015115731765933488273881059259173651847367586
00717786881848694963119917080234343393438632241104852
58009551230229914776980932747760519270603805313338263
75120534463741477208577693040311951483520936643946758
72365294696107512311961830988946821046132329436035031
14593168911892 49

1997

Johannes Gutenberg Stiftungsprofessur

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Google may unveil a powerful quantum computer by end of 2017

2 September 2016 | By Sebastian Moss

Johannes Gutenberg Stiftungsprofessur

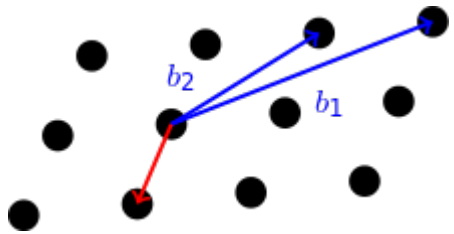
Langfristiger Schutz ist möglich

http://www.crossing.tu-darmstadt.de

Johannes Gutenberg Stiftungsprofessur

Post-Quantum Cryptography

3179526881036662712547379085979709839119790828652543507736401128590510438382632507968446475666470736765037698350040734989120408350361119844369827869651498796736654117936223083038631384645332380078749777062290203703984426916486099363952209642499739231832242823262429388312437906163176507342320461004280137879967546128234413259882008909669991881742777224061960485068828406517329900151157317659334882738810592591736518473675860071778688184869496311991708023434339343863224110485258009551230229914776980932747760519270603805313338263751205344637477208577693040311951483520936643946758723652946961075121961830988946821046132329436035031145931689118924 9

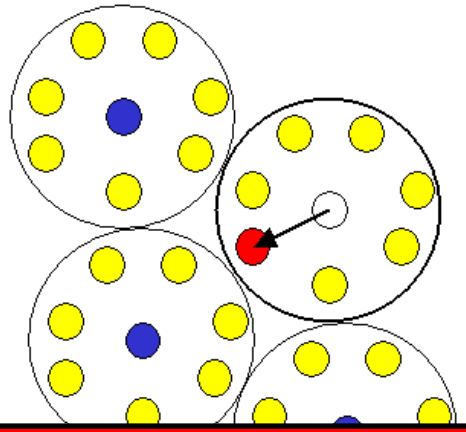


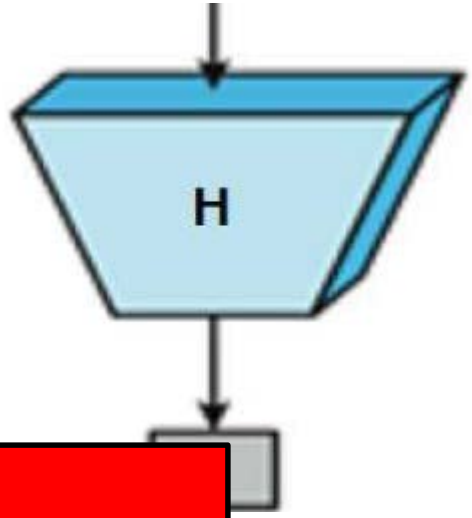
$$\bar{X}_i = \frac{1}{n_i}\sum_{j=1}^{n_i} X_{ij},$$

$$A_i = \sum_{j=1}^{n_i}(X_{ij} - \bar{X}_i)(X_{ij} - \bar{X}_i)',$$

$$S_i = \frac{1}{n_i - 1}A_i,$$

$$\tilde{S}_i = \frac{1}{n_i}S_i,$$



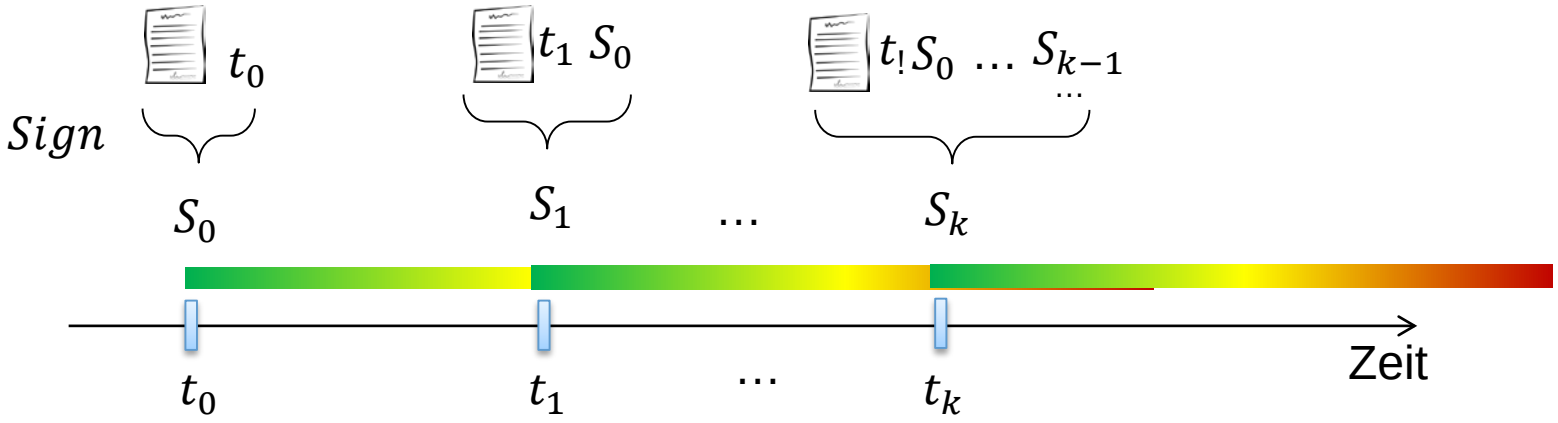


Kein Beweis für Quantencomputerresistenz

Johannes Gutenberg Stiftungsprofessur

Langzeit-Integrität und Authentizität

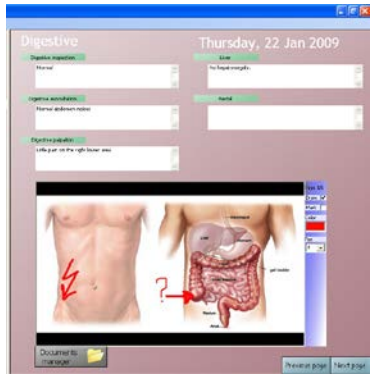
Gültigkeit von Signaturen kann verlängert werden



Kann Gültigkeit von Verschlüsselung verlängert werden?


NSA Datenzentrum in Utah:
Bis zu 140 Terabyte für jeden Menschen auf der Welt
Angreifer können verschlüsselte Daten jetzt speichern und später entschlüsseln

Langzeit-Vertraulichkeit

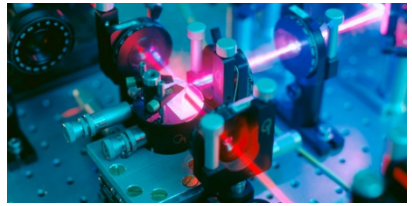


Data **in transit**

Quanten-Schlüsselaustausch [BB84]

+

One-Time-Pad-Verschlüsselung [Shannon 48]



Informationstheoretisch sichere Vertraulichkeit

Caesar Chiffre 60 v. Chr.

K	R	A	N	I	C	H

Caesar Chiffre 60 v. Chr.

K	R	A	N	I	C	H
N						

Caesar Chiffre 60 v. Chr.

K	R	A	N	I	C	H
N	U					

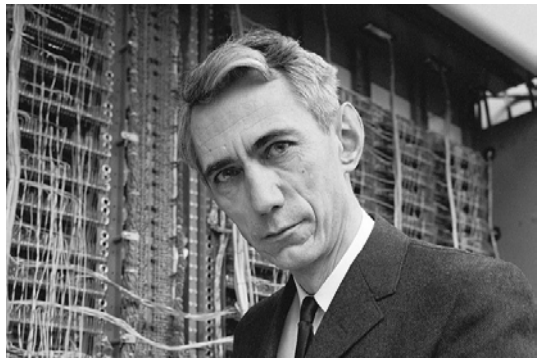
Caesar Chiffre 60 v. Chr.

K	R	A	N	I	C	H
N	U	D				

Caesar Chiffre 60 v. Chr.

K	R	A	N	I	C	H
N	U	D	Q	L	F	K

Perfekt sichere Verschlüsselung 1948



Claude Shannon (1916 – 2001)

k	r	a	n	i	c	h

Schlüssel wird zufällig gewählt

k	r	a	n	i	c	h
3	13	15	3	21	20	22

Schlüssel wird zufällig gewählt

k	r	a	n	i	c	h
3	13	15	3	21	20	22
N	E	P	Q	D	W	D

Schlüssel wird zufällig gewählt

N	E	P	Q	D	W	D

N	E	P	Q	D	W	D
3	13	15	3	21	20	22

N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h

N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h

N	E	P	Q	D	W	D
12	10	23	24	3	5	0

N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h

N	E	P	Q	D	W	D
12	10	23	24	3	5	0
b	u	s	s	a	r	d

N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h

N	E	P	Q	D	W	D
12	10	23	24	3	5	0
b	u	s	s	a	r	d
24	0	4	8	19	22	16

N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h

N	E	P	Q	D	W	D
12	10	23	24	3	5	0
b	u	s	s	a	r	d
24	0	4	8	19	22	16
p	e	l	i	k	a	n

N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h

N	E	P	Q	D	W	D
12	10	23	24	3	5	0
b	u	s	s	a	r	d
24	0	4	8	19	22	16
p	e	l	i	k	a	n
k	o	l	i	b	r	i

N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h

N	E	P	Q	D	W	D
12	10	23	24	3	5	0
b	u	s	s	a	r	d
24	0	4	8	19	22	16
p	e	l	i	k	a	n
3	16	4	8	2	5	21
k	o	l	i	b	r	i

N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h

Jeder Klartext mit sieben Buchstaben ist möglich

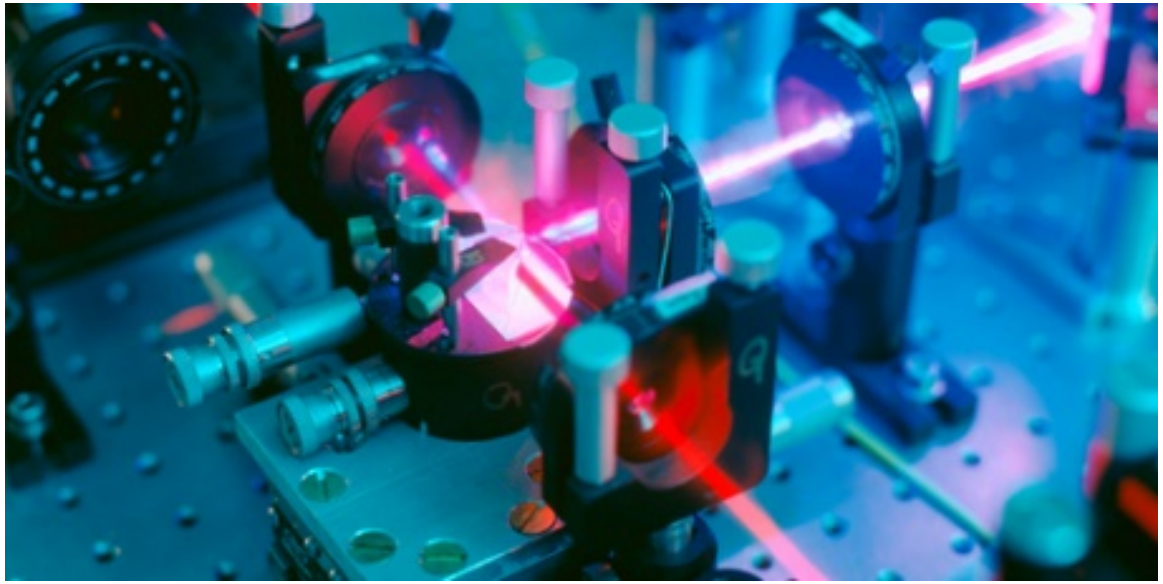
N	E	P	Q	D	W	D
12	10	23	24	3	5	0
b	u	s	s	a	r	d
24	0	4	8	19	22	16
p	e	l	i	k	a	n
3	16	4	8	2	5	21
k	o	l	i	b	r	i

N	E	P	Q	D	W	D
3	13	15	3	21	20	22
k	r	a	n	i	c	h

Theorem von Shannon:
Der Angreifer lernt nichts
aus dem Schlüsseltext

N	E	P	Q	D	W	D
12	10	23	24	3	5	0
b	u	s	s	a	r	d
24	0	4	8	19	22	16
p	e	l	i	k	a	n
3	16	4	8	2	5	21
k	o	l	i	b	r	i

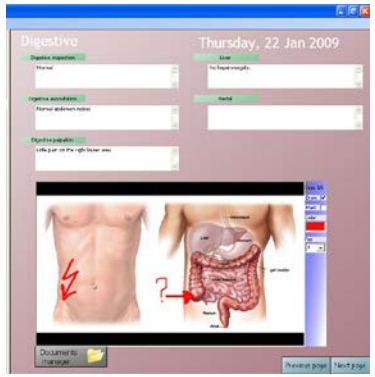
Quantenschlüsselaustausch




Beijing
Jinan
Hefei
Shanghai
CHINA
Area of
enlargement

EU: Quantentechnologie-Programm mit einem Budget von 1 Mrd. Euro vorgestellt

Das Flaggschiff-Projekt soll Anwendungen der Quantenphysik voranbringen – etwa Quantenkommunikationsnetzwerke, hochpräzise Atomuhren, Gravitationssensoren und Quantensimulatoren zur Entwicklung neuer Materialien und Quantencomputer.

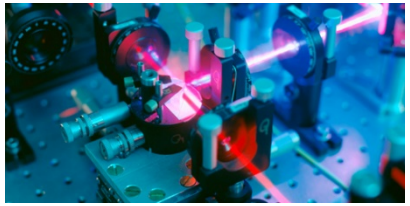


Data **in transit**

Quanten-Schlüsselaustausch [BB84]

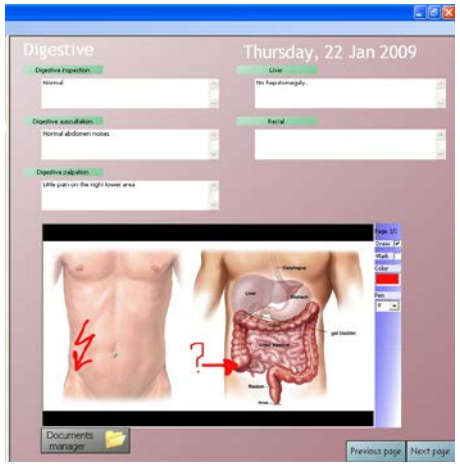
+

One-Time-Pad-Verschlüsselung [Shannon 48]



Informationstheoretisch Sichere Vertraulichkeit

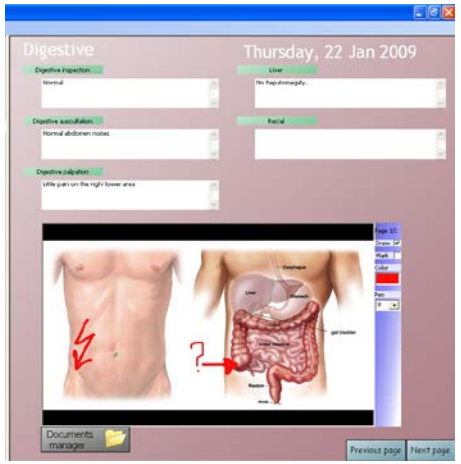
Langzeit-Vertraulichkeit



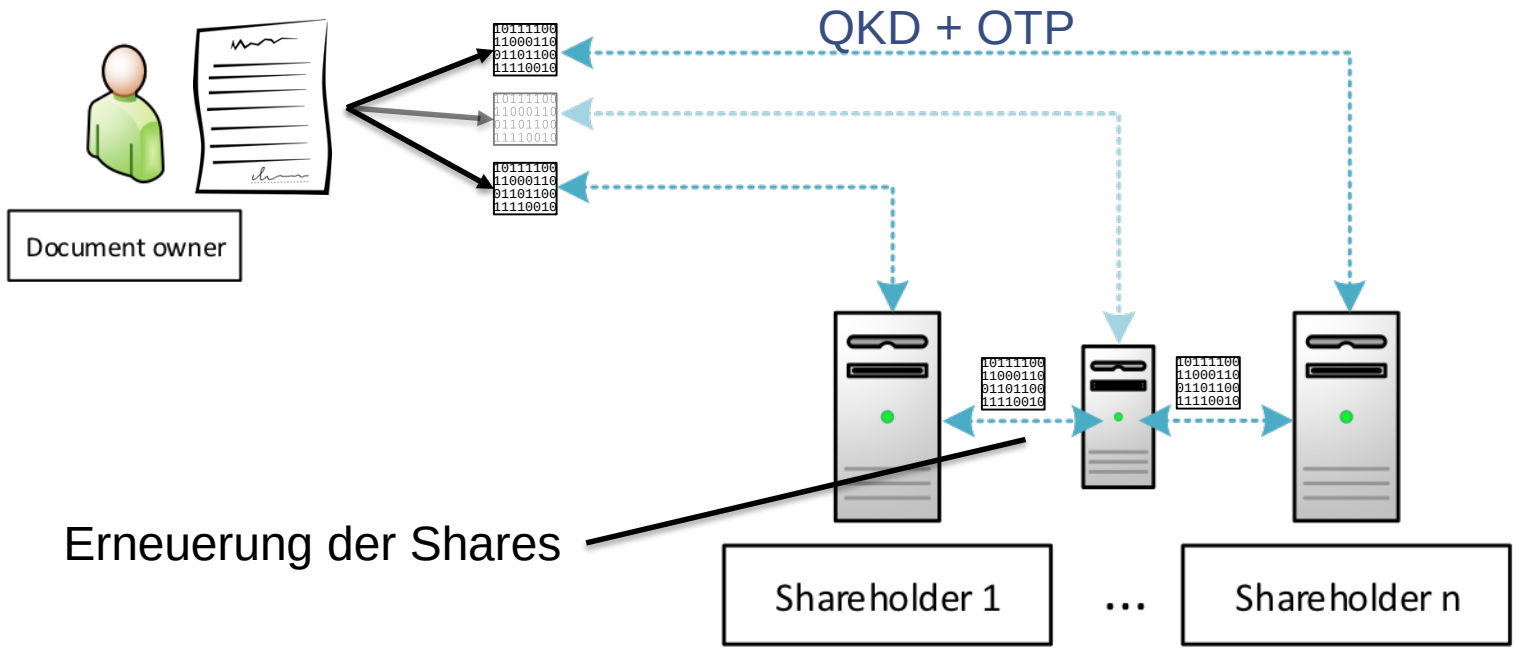
Data **at rest**

One-time pad?


03003802 996CB7BA 0EG0161B G0021C06
BA7CE203 G0030200 01208600 37D14D00
1B7125G0 024FG002 53D03C00 AD722500
BD03C00 887525C1 01A07700 37D14D00
B7125G0 024FG002 53D03C00
BD03C00 887525C1
F4F3D41 4242434E
6C2F4F 553D4553
425604
003042
2254F1
3ECAA CB3EE8EF DF038D7F A14217
2AA4D 04143B75 4F571C83
7DED9 B57C659E C820EE07 FA49F
96DB 7D7F743D 9A36DD29 454E0
014D 410800C8 9A54E072

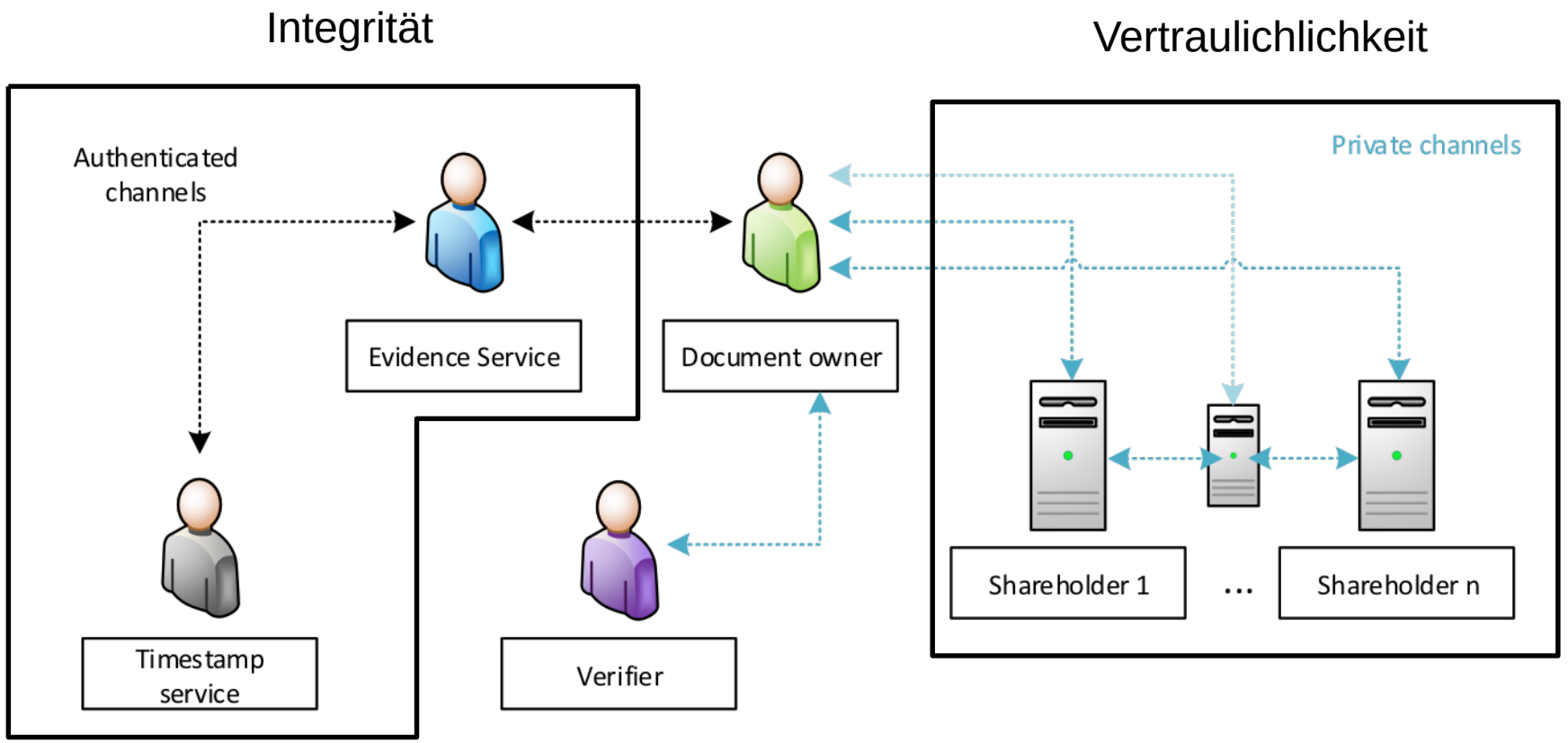

Digestive
Thursday, 22 Jan 2009
Documents manager
Previous page
Next page

Proactive Secret Sharing

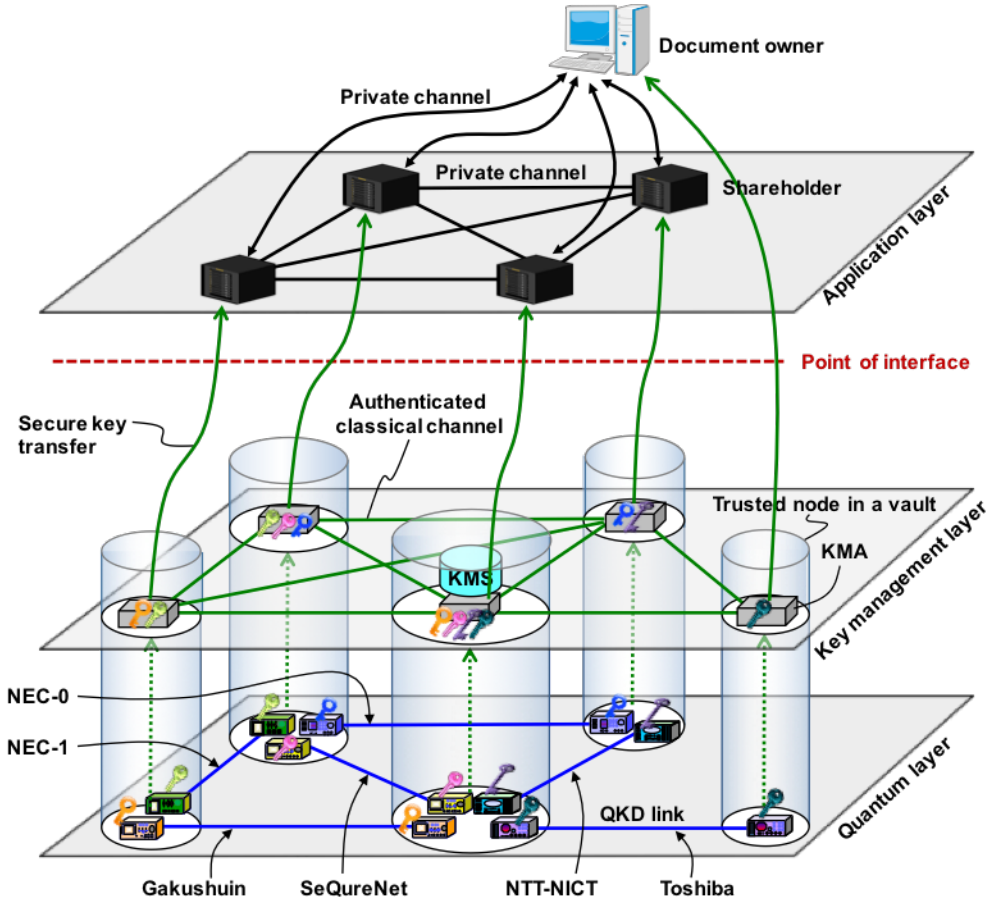


Johannes Gutenberg Stiftungsprofessur

2016 LINCOS in Kooperation mit NICT Japan


Integrität
Vertraulichlichkeit
Authenticated channels
Evidence Service
Document owner
Timestamp service
Verifier
Private channels
Shareholder 1
...
Shareholder n

Tokyo QKD Network of NICT



Link	Distanz (km)	Key Rate (kbit/s)
NEC-0	50	200
NEC-1	22	200
Toshiba	45	300
NTT-NICT	90	10
Gakushuin	2	100
SeQureNet	2	10

Zeit für Quantenschlüsselaustausch

Johannes Gutenberg Stiftungsprofessur

Datenmenge	Zeit
1 KB	0.027 Sekunden
1 MB	4.45 Minuten
1 GB	7.41 Stunden

Johannes Gutenberg Stiftungsprofessur

Fazit:

Langzeitschutz von Integrität und Vertraulichkeit ist nötig und möglich.

Weitere Forschung ist nötig.


LERNENDE MASCHINEN 02.05.2017
INDUSTRIE 4.0 23.05.2017
SPRACH-DIALOGE 09.05.2017
KÜNSTLICHE INTELLIGENZ
KI
BIG DATA 13.06.2017
TEAM-ROBOTIK 30.05.2017
AUTONOME SYSTEME 16.05.2017
ALTERS-ASSISTENZ
SMART SERVICE 27.06.2017
SICHER-HEIT 20.06.2017
EMOTION & VERHALTEN

Vielen Dank für Ihre Aufmerksamkeit

Johannes Gutenberg Stiftungsprofessur

TECHNISCHE UNIVERSITÄT DARMSTADT