

State-of-the-Art-Sicherheitsmaßnahmen bei Verschlüsselung und Authentifizierung

T. I. S. P. Community Meeting, Frankfurt 11. November 16

Herr Dennis Scherrer

BLUESITE Beratungsgesellschaft für die Informationstechnologie mbH



Themen

- Verschlüsselung
- Authentifizierung
 - Bruchsicherheit
 - Marktdurchdringung
 - gängige Verfahren

10. - 11.11.201 T.I.S.P. Community Meeting 3

Fingerabdrücke in Freizeitparks (Walt Disney World)

<https://epic.org/privacy/themepark>



Wie die NSA Verschlüsselungen knackt

<https://www.welt.de/wirtschaft/article119782731/Wie-die-NSA-Verschluesselungen-knackt.html>

Gemalto ./ NSA zu SIM-Karten

<http://arstechnica.com/security/2016/10/how-the-nsa-could-put-undetected-trapdoors-in-millions-of-crypto-keys>

<http://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx>

National Institute of Standards and Technology, Cryptographic Toolkit

<http://csrc.nist.gov/groups/ST/toolkit/index.html>

European Union Agency for Network and Information Security (ENISA),

Algorithms, key size and parameters report

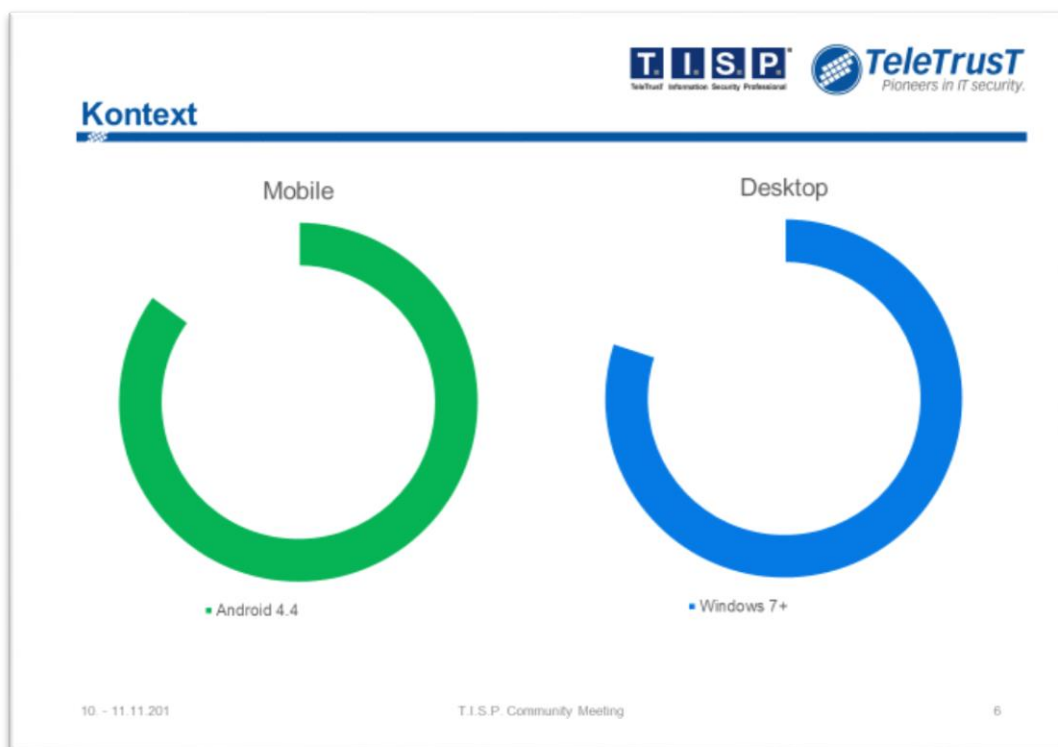
<https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data/cryptographic-protocols-and-tools>

Bundesamt für Sicherheit in der Informationstechnik (BSI), TR-02102-1

"Kryptographische Verfahren: Empfehlungen und Schlüssellängen"

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Signaturbestaetigung/02102_pdf.html

Damien Giry (<http://www.uclouvain.be/crypto/people/show/6>), <https://www.keylength.com>



Windows Desktop <https://www.netmarketshare.com/operating-system-market-share.aspx> Oktober 2016 Windows 7+ 80%+

Android Mobile <http://www.idc.com/prodserv/smartphone-os-market-share.jsp> 85%+,
https://de.wikipedia.org/wiki/Samsung_Galaxy_S5

Firefox <https://www.mozilla.org/de/firefox/sync/>

Chrome <https://www.google.com/intl/de/chrome/browser/features.html#signin>
(<http://gs.statcounter.com/#browser-eu-monthly-201510-201610>)

KitKat (Android 4.4)
<https://source.android.com/security/encryption/full-disk.html>

iOS Security Guide
https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Bitlocker und Bitlocker2Go (USB-Stick)

AES-CBC + diffuser

Option „with Diffuser“, eine Entwicklung von Microsoft, wurde zu Gunsten von Hardwarebeschleunigern in Build 9200 wieder entfernt. Microsoft wählte die Option ursprünglich für Performance.

AES 128 oder 256 (symmetrischer Algorithmus, eine Blockchiffre) - #10240



Dennis Scherrer Technical Summit 2015, Darmstadt

Dennis Scherrer Technical Summit 2015, Darmstadt

<http://www.microsoft.com/germany/technical-summit/speaker-2015.aspx>

Maßnahmen Verschlüsselung

- M1 = Smartphones, USB-Sticks und besonders exponierte dauerhafte Speicher verschlüsseln 128-256 Bit (kein OS vor KitKat oder Win. Vista)
- M2 = PKI-Zertifikate (Webserver, Benutzer, Client-APS, etc.) Schlüssellänge RSA 2048-3072

NOC = erhöhtes Risiko

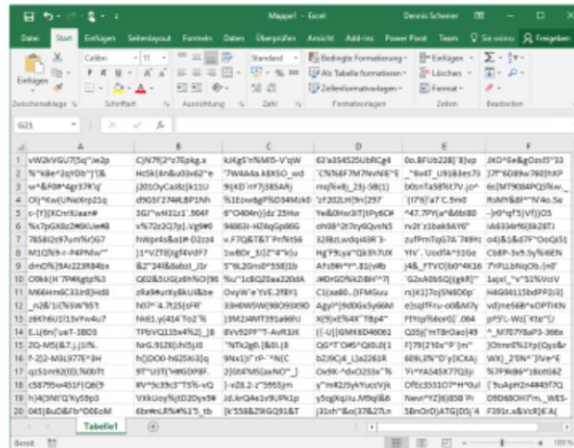
WinZip <http://www.winzip.de/wzfeatures-protect.htm>

Dropbox <https://www.dropbox.com/security#protection>

Microsoft Office Dateischutz

<https://support.office.com/de-de/article/Festlegen-eines-Kennworts-zum-Öffnen-oder-Ändern-eines-Dokuments-einer-Arbeitsmappe-oder-einer-Präsentation-EF163677-3195-40BA-885A-D50FA2BB6B68>

Komplexe Kennwörter



	A	B	C	D	E	F
1	vW2KVGU75q"3a2p	C/N7(2"270p4g.x	uUg5YhMS-VjvW	62x5552558Cg8	6a.BFub228)8)ep	JKD*Ea&g0e05"23
2	%*8e"2q08"J)5&	H08(4n&a03a62"e	77WAAAa.88X50_und	C/N8477M7NvN8"E	_"8u4T_u988e57)	37F6089w760P8P
3	w849M*4p17K7	2010YCaR0(x110	9)4D"v758548)	m0h+8L_23)58(1	00on155887V_jor	6e2u79040Q29w_
4	O194u01hu0p22g	d90377M8.BP248	%11+u0gP803M686	7F2123H3h1257	(178)87C.5m0	8uAm88"7V8u.5a
5	e-[5]8K20k8e#	3G7uH31u1.304F	8"0404e)8r.258e	7u888u03T)PydCK	"42.79)u"6d880	-39"q73(V1)05
6	%7p0X82M0u0e#	v%72207j).vg98	94863+408p86G	en88"2r7y0QvN5	rv2T.12a884V0"	u8334W0(8a28T)
7	76580297umf0y67	H8p8a8a8P.0224	v.F70&T&T.P8e58	12881u0q48K.3	zu9m7q576.789e	o4)8&877"0uQ51
8	M1029+88Pdu"	11"v270g54v977	2u80_1)2"4"X'u	hg78g8"08307uX	7H'.u0d8A"330a	CM8P.8v5.5y%66N
9	4u0R7M4228848a	8L"248&du01.JU	77uL20r0P23830	A708"77"81v86	748_77V030P"4828	77P0L8u02u.3eF
10	08847H.788g8r83	Q0285u0g8h80)95	%u"1d020x22048	48028u288"77	52u8850)8887	1a9u_"%325v0v
11	M668m0C33x048	2k88u8u88u88e	0v9W"e.YV8.2883	C1u888_8F8G8u	r1K170)9880p	88881158dP828
12	u0&10N8W951	h07"4.7125)8F	8948W5W9809080	Agp7"8808x7y68M	8u87Fru-088M7y	vd7ne588v8P818N
13	2848u0113v7u4u7	8881.y414.702.76	13M248M735888u	X05vE4X"78p4"	FT8p88805) 084	gP3L.W0(X8"U)
14	L488(u87.2803	778vQ138w7u2_8	8v85277"7.Au81X	(-U)0888048881	Q25(8778G8u)48	^_N75788P.3888
15	20.888877j8u7	8v8.9120u8888	7878g8)8818	Q5"7"08"Q88811	77787788"8"j8u7	308v88288888888
16	8.22.8888877"34	h2008-h258888	98u1)7"8P-"88C	h2888u_1a22888	688838"0.y0C8A	W8L_278u"778vE
17	q58788888888888	87"u8178888888	22888888888888	0u88"8u02888"76	77"888888888888	778888888888888
18	u88788888888888	8v"3838"735-vQ	7+28.2.8"388888	77"888888888888	08888888888888	778888888888888
19	h48888888888888	V88u8888888888	88888888888888	77888888888888	88888888888888	888888888888888
20	043)8u0888888888	88888888888888	88888888888888	88888888888888	88888888888888	888888888888888

Jörg Riether „Fast aussichtslos“ iX vom Juli 2016, Heise Verlag

Software „Password List Generator 2“ von Arunas Skirius

<http://www.arunass.net>

Smartcard-Anmeldung



Smartcard für die Benutzeranmeldung

Smartcards mit verschiedenen COS

<http://www.cryptoshop.com>

Datenhaltung Bio-Daten Authentifizierung



[http://winfwiki.wi-fom.de/index.php?title=Der neue Reisepass im Lichte des Datenschutzes](http://winfwiki.wi-fom.de/index.php?title=Der_neue_Reisepass_im_Lichte_des_Datenschutzes)

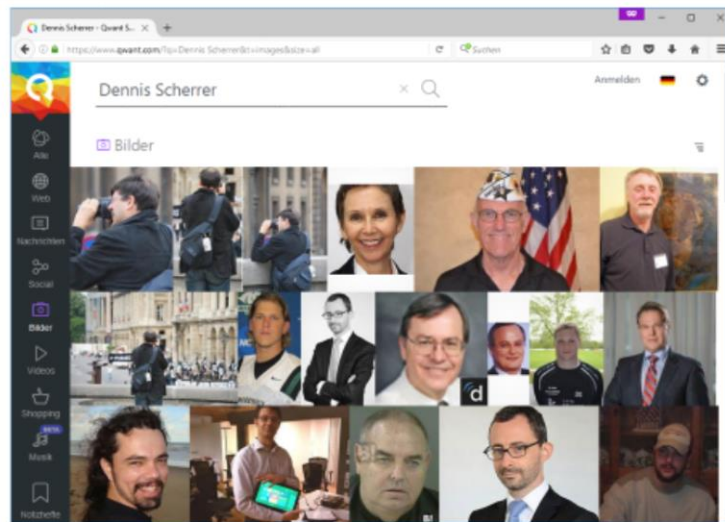
Signaturwaffe mit Fingerabdruckerkennung

<https://de.wikipedia.org/wiki/Signaturwaffe>

Microsoft Halo

<https://technet.microsoft.com/en-us/itpro/windows/keep-secure/manage-identity-verification-using-microsoft-passport>

Gesichtserkennung



<https://www.wired.com/2016/10/cops-database-117m-faces-youre-probably/>

Ausblick

- neue Kryptografie
- komplexe Kennwörter
- Gesichtserkennung

NSA Quantum Computer FAQ

<https://www.iad.gov/iad/customcf/openAttachment.cfm?FilePath=/iad/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/assets/public/upload/CNSA-Suite-and-Quantum-Computing-FAQ.pdf>

Kreditkarte mit eingebautem Fingerabdruckleser

<http://zwipe.com/products>



Digitalisierung im September 2016 Stuttgart-Mitte

Information technology - Security techniques, <http://www.iso.org>

- Security requirements for cryptographic modules (ISO/IEC 19790:2012)
- Test requirements for cryptographic modules (ISO/IEC 24759:2014)
- Verification of cryptographic protocols (ISO/IEC 29128:2011)