

T.I.S.P. Community Meeting

Berlin, 14. - 15.11.2017

Sicherheit mit Windows-Bordmitteln

Dennis Scherrer, BLUESITE

Windows überall

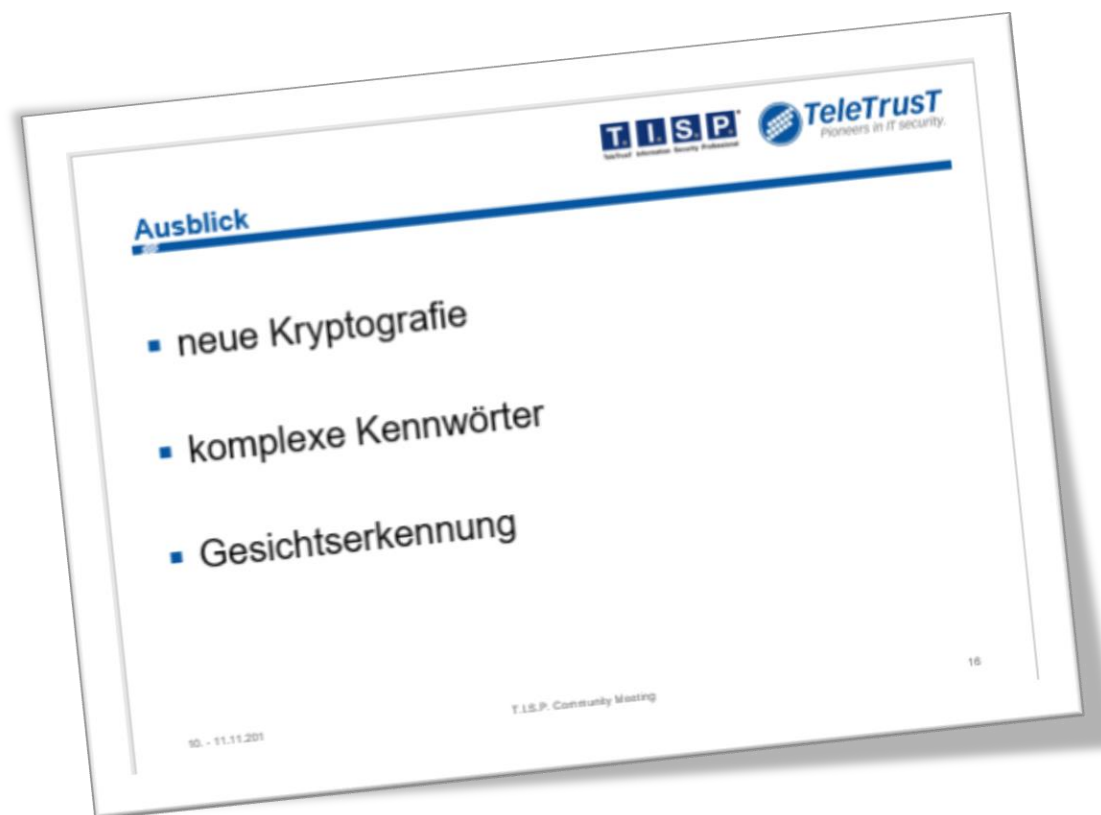


Stuttgart-Mitte im Oktober 2014

Schutzziele

- Authentifizierung (Mensch)
 - Windows Hello Business
- Integrität (Arbeitsplatzrechner)
 - AppLocker

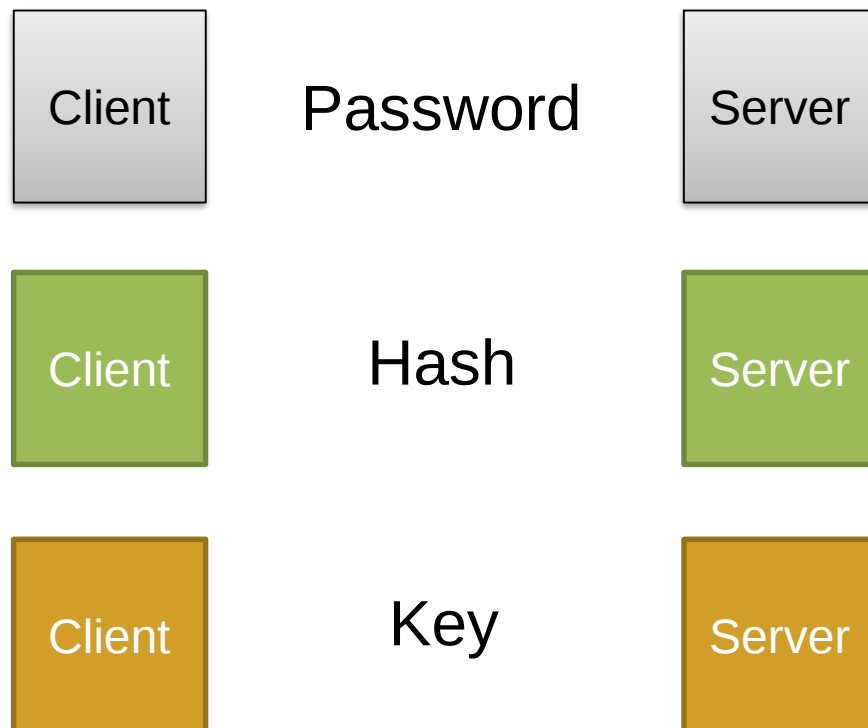
Rückblick / Ausblick



T.I.S.P. Community Meeting 2016

- IBM bietet Quantencomputer als Web Service
- Microsoft kündigt VST Erweiterungen für Quantencomputer an
- Microsoft veröffentlicht Roadmap für das Ende der Kennwörter
- Windows 10 und iPhone X mit Gesichtserkennung

Windows Anmeldung



- Integrated Windows authentication (NTLM, Windows NT Challenge/Response authentication)
- Windows Build 2195 (17.02.2000) Microsoft Windows 2000 Public Key Infrastructure
- Kerberos v5 Standard, aber ...

Kennwörter

Mappe1 - Excel Dennis Scherrer

Datei Start Einfügen Seitenlayout Formeln Daten Überprüfen Ansicht Add-Ins Power Pivot Team Sie wüns Freigeben

Einfügen Zwischenablage

Schriftart Ausrichtung Zahl Formatvorlagen Zellen Bearbeiten

G21

	A	B	C	D	E	F
1	vW2kVGU7{5q~Je2p	C)N7f(2^z7Epkg.x	kJKgS'n%MI5-V'qW	63'a3S4525UbRCg4	0o.BFUb22B}`8}vp	JXO^Ee&gOzsl5~33
2	%~kBe^2qYDb~){&	Hc5k{4n&u03x62~e	'7W4A4a.k8XSO_wd	`C%8F7M7NvNIE~E	_~6v4T_U91B3es73	}7f~6D89w760}hXP
3	w^&F0#^4gr37R'q'	j201OyCaJ8z}k11U	9lJKD'nY7j385ARj	mq%v8j_23j-5B(1)	b0snTa58%t7V.jo^	6s{MT9084PQ5%w._
4	Olj^Kw(UNeXrp21q	d9G5l'274#LBP1Nh	%1Eow6gP%D34Mzk0	'zF202LH{9n{297`	`(I7'6'a7'C.9m0	RsMY&8l^N'4o.Se
5	c-{Y}{XCnrXJaan#	3GJ~wH31z1'.904F	6~O404n){dz`25Hw	Ye&0Hw3IT)tPy6C#	^47.7PY(a^&6bl80	-}r0^qf'5)Vf))O5
6	%s7pGX8zZ#6KUe#B	v%72z2Q7p}.Vg9#0	94863i-HZ4qGp86G	oh08^2t7cy6QvsN5	rv2t`z1bak9AY6"	iA6334rf6{6kZ6TJ
7	7858I2s97um%r}G7	hWpr4s&a1#-D2zz4	v.F7Q&T&T'Pn%tS6	32lBzLwdqi43R`3-	zufPmTqG7A`749Yc	o4)&1&d7F~OoQi51
8	M1Q%9-r-P4PNlw~"	)1^VZT8)lGf4VdF7	1wBDR_3j}Z~4~k{u	Hg'F9Lya~Qk3h7UX	YIV.`UodfA^31Ge	Cb8P-3v9.Sy%i6EN
9	dmD%}9Ai223R84bx	&2~24l&8abzl_J1r	S~6L2Gns0^558}1b	AFs9#i^Y^A.81(v#b	j4&_FTVO)b0^4K16	7rPLlbNqOb.{n0'
10	O9kk{H`7P#Xgtp%3	Q02&5UG(z6h%O{96	%u~1cBQZ0aa220dA	J#DrGD%kZIBH'^7(	`G2xA0bSQ){gkR}~	1ajxl_~v~S1VciV
11	M66Hm6C33Jr8}Hd8	zRa9#urXyBkUI&be	OvyW'e`tVE.2fBY1	C1(aa80..{IFMGuu	rs)K1}7ojSN6D0p`	H4G04115bdPP2J3}
12	_n2&'1i{(%SW'95't	h07^4.7t25(sFR'	33H0W5W(98O93X9D	AgyI^l)9d0Gx5y66M	e}sqlfFru-o0&M7y	vd)neS6B^xOPTIKN
13	z6Kh6U1l13vYw4u7	hk61.y(414`To2`%	)3M2J4MT391a66hJ	X(9)xE%4X"TBp4~	FtYcp%6orG}`.064	pF5'L-Wz{'Kte~J
14	E.L{6n{'ueT-3BD3	TPbVQ135x4%2)_8	8Vv92PF~T-Avr3JK	{{-U)}GMK6D46061	Q35j{('mT8rOao)49	^_M707Y8aP3-366x
15	ZQ-M5(&7.j.j1l%.	NrG.9126jJhI5jJ0	'NTk2go.{&0l.(8	QG^T'O^S^QI0L0(1	F}79{2't0x~P`{m~	}OtmrE%1Yp{Qyz&r
16	f-2j2-M3L977E^3H	h{DO0-h625Xi3}q	9Nx1j)l'p~^N{C	bZJ9Cj4_L)a2261R	609L3%~D'y{ICXAJ	WX)_2'0N^}Ive^E
17	qz51m92{0}L%ObTt	9T~U3T('H#GDP8F.	2{Gt4'MS{axNO~_}	Ox9X-^dxO233x"~%	'Fi^YA545X77Q3ji	%7F9kB6^z8otG6Z
18	cS8795w451F(Q6{9	#V^5c39c3~TS%-vQ	}-vZ8.2-z~59SSjm	y~m#2JsykYuccVjk	OfEc353107^H^0ul	{`9uApH2n4#45f7Q
19	h}4(5Nt'Q'KyS9p3	VXkUoy%jtD2Dyx9#	Jd.krQ4e1v9UPk1p	y5cgXqJiu.M9ql&6	Nevi^YZj6)85B`Pi	D9D68OH7'm._WES-
20	045)BuD&Fb^D0EoM	6br#nLR%#%1'5_tb	{k'558&Z9IGQ91&T	j31sh~&o(37&27Ln	5BnOrd)ATGjD5j`4	F391r.x&VcR}6^A{

Tabelle1

Bereit

Smartcard in Windows R.I.P.



Smartcard für die Benutzeranmeldung

Smartcard-Einstellungen

Einstellung

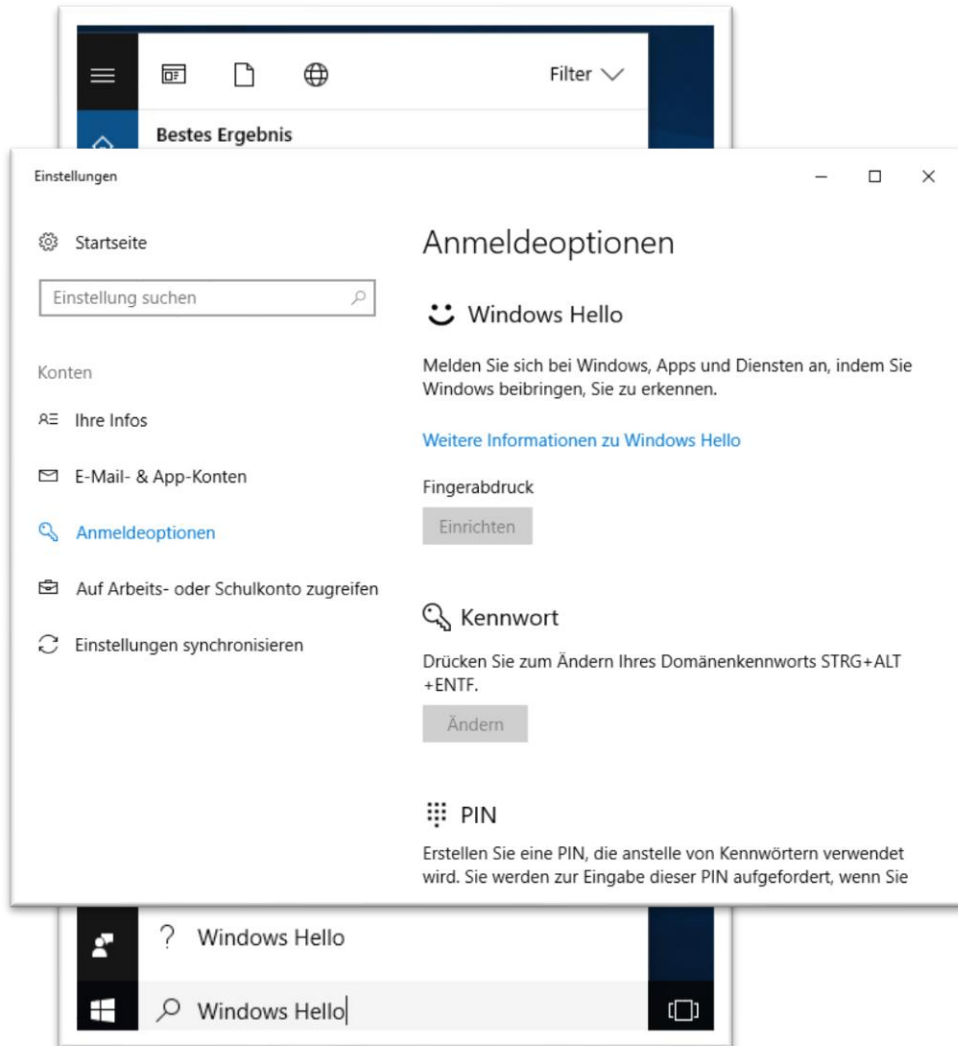
-  Zertifikate ohne Zertifikatattribut für erweiterte Schlüsselnutzung zulassen
-  Anzeige des integrierten Bildschirms "Blockierung der Smartcard aufheben" bei der Anmeldung zulassen
-  Für die Anmeldung gültige Signaturschlüssel zulassen
-  Zertifikate mit ungültiger Zeitangabe zulassen
-  Zertifikatpropagierung von der Smartcard aktivieren
-  Bereinigung von Stammzertifikaten konfigurieren
-  Stammzertifikatpropagierung von der Smartcard aktivieren
-  Rückgabe von Nur-Text-PINs durch Anmeldeinformationsverwaltung verhindern
-  Verwendung von ECC-Zertifikaten für Anmeldung und Authentifizierung zulassen
-  Doppelte Anmeldezertifikate filtern
-  Lesen aller Zertifikate von der Smartcard erzwingen
-  Zeichenfolge bei blockierter Smartcard anzeigen
-  Im Zertifikat gespeicherten Antragstellernamen bei der Anzeige umkehren
-  Smartcard-Plug & Play-Dienst aktivieren
-  Benutzer bei erfolgreicher Smartcard-Treiberinstallation benachrichtigen
-  Benutzernamenhinweis zulassen

- Schattenkennwörter
 - Windows Server 2016 Funktion
 - Kompatibilität
- Hashes
- PIN-Speicherung
- Teure Prozesse
 - Provisionierung (mit Betriebsausweis)

Windows Hallo - Features

■ Merkmale

- PIN
- Fingerabdruck
- Gesicht



Überlegungen zu Windows Hallo

 Windows Hello

Melden Sie sich bei Windows, Apps und Diensten an, indem Sie Windows beibringen, Sie zu erkennen.

[Weitere Informationen zu Windows Hello](#)

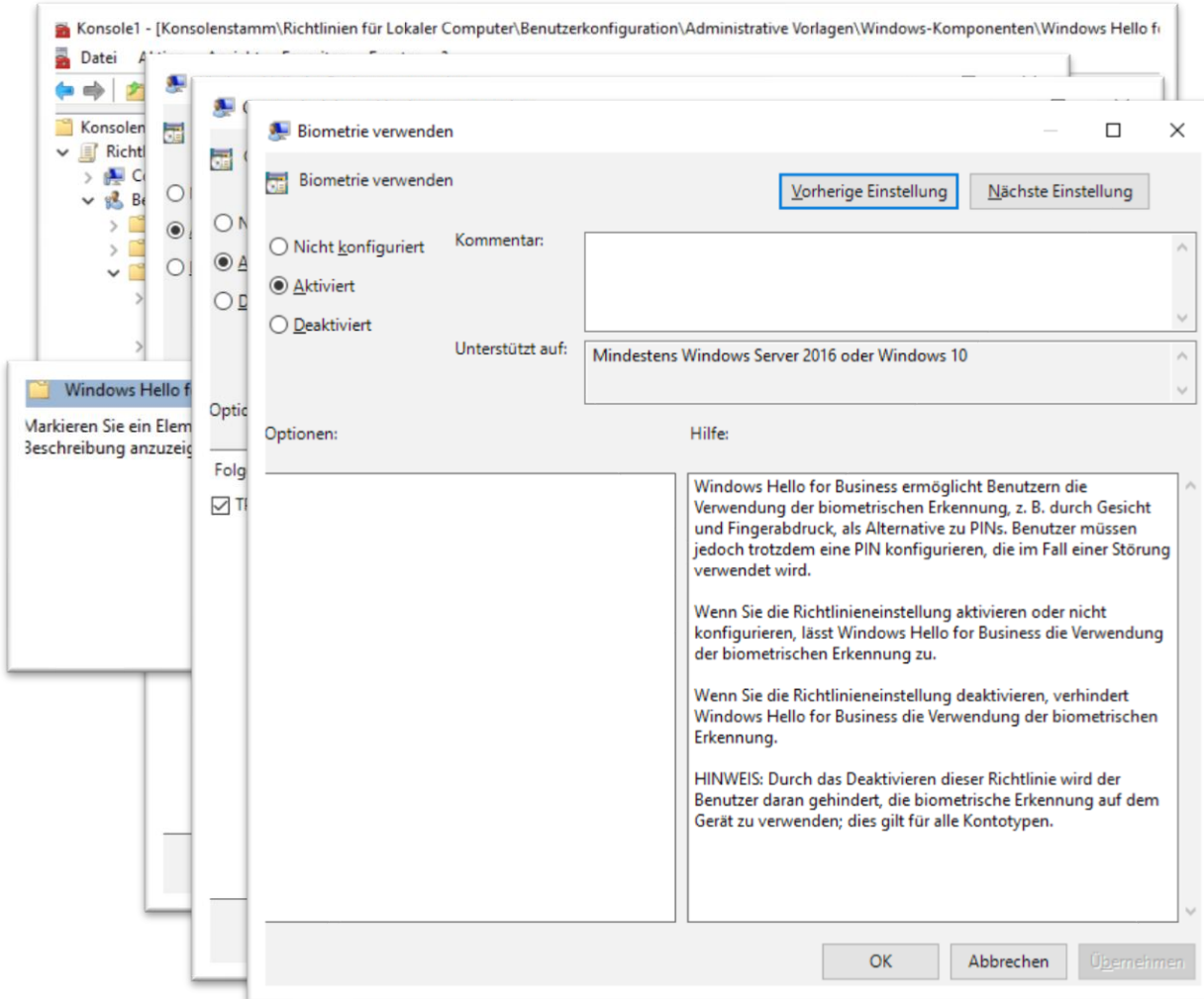
Fingerabdruck

 Kennwort
 Drücken Sie zum Ändern Ihres Domänenkennworts STRG+ALT+ENTF.

 PIN
 Erstellen Sie eine PIN, die anstelle von Kennwörtern verwendet wird. Sie werden zur Eingabe dieser PIN aufgefordert, wenn Sie

- Komplexität des obligatorischen PIN
 - sicherer als ein komplexes Kennwort?
 - seltenere Verwendung
- Smartphone-App für Initialisierung
 - Prozesse für Smartcard Provisionierung
- Windows-Plattform Angriffe

Richtlinien zur Konfiguration



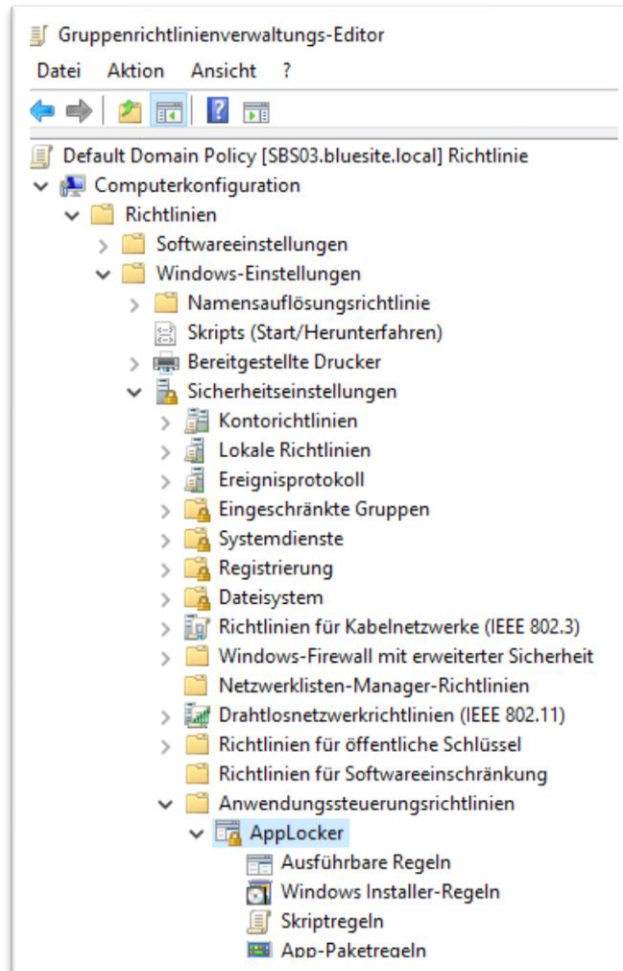
- Benutzer-Richtlinie aktivieren
- Computer-Richtlinie
 - TPM erforderlich, 1.2 aussperren
 - Biometrie aussperren
- Windows 10, Server 2016
 - Build 1607-1703, AD Schema

Schutzziele

- Authentifizierung (Mensch)
 - Windows Hello Business
- Integrität (Arbeitsplatzrechner)
 - AppLocker

Windows Angriffe

Anwendungssteuerung (AppLocker)



- Richtlinien für Anwendungen
 - Ausführung
 - Installation
 - Scripting
 - Pakete

Ausführungsregeln

Ausführbare Regeln erstellen

Referenzdatei:

C:\Program Files\Windows NT\Accessories\word Durchsuchen...

Beliebiger Herausgeber

Herausgeber: O=MICROSOFT CORPORATION, L=REDMOND, S=

Produktname: MICROSOFT® WINDOWS® OPERATING SYSTEM

Dateiname: WORDPAD.EXE

Dateiversion: 10.0.0.0 und höher

☐ Benutzerdefinierte Werte verwenden

Regelbereich:

Betrifft nur die angegebene Dateiversion.

Anwendungen die ausgeführt werden dürfen filtern

- Negativ/Positiv
- Zertifikat (Herausgeber)

Prozesse für Anwendungen

- Installation
 - Updates
 - Patches
 - Quellen
- Wie lassen sich Prozesse beschleunigen?
 - Standardsoftware
 - Vertrauenswürdige Quellen
 - Prüfung auslagern

Windows Store Richtlinien

■ Microsoft Store für Unternehmen

Einstellung

-  Automatisches Herunterladen von Updates auf Windows 8-Computern deaktivieren
-  Automatisches Herunterladen und Installieren von Updates deaktivieren
-  Deaktivieren des Angebots zum Update auf die aktuelle Version von Windows
-  Alle Apps aus dem Windows Store deaktivieren
-  Store-Anwendung deaktivieren
-  Nur privaten Store in der Windows Store-App anzeigen



Digitalisierung im September 2016 Stuttgart-Mitte