Otto-Friedrich-Universität Bamberg

Rollout-Plan für Passkeys

82. DFN-Betriebstagung 25./26.03.2025

Ausgangpunkt und Ziel

- Beschluss der UL zur Einführung auf Empfehlung CIO
- Ziel:
  - Passkey userless ➔ Passwörter sollen möglichst bei allen Logins verschwinden, bei Logins aus dem Internet komplett
  - Keine Verwendung von OTPs für normale user ➔ OTPs stehen in Kritik bezüglich Security (fertige Angriffe username + password + otp)
  - Absicherung E-Mail für Exchange on premise (Vortrag 2)

Umsetzung

- Konzentration auf Webanwendung und E-Mail (2. VT)
- eduMFA und Shibboleth mit fudiscr-Plugin, unterstützt Passkey userless
  https://doku.tid.dfn.de/user:hofmann_fu-berlin.de
- Passkey im TPM, d.h. keine zusätzliche Hardware
  - Windows mit Windows Hello (nicht Windows Hello for Business)
  - MacOS
  - Fallback Desktop-OS: KeeepassXC
  - Android / IOS
- Passkey auf Yubikey / Nitrokey funktioniert (kein Support)

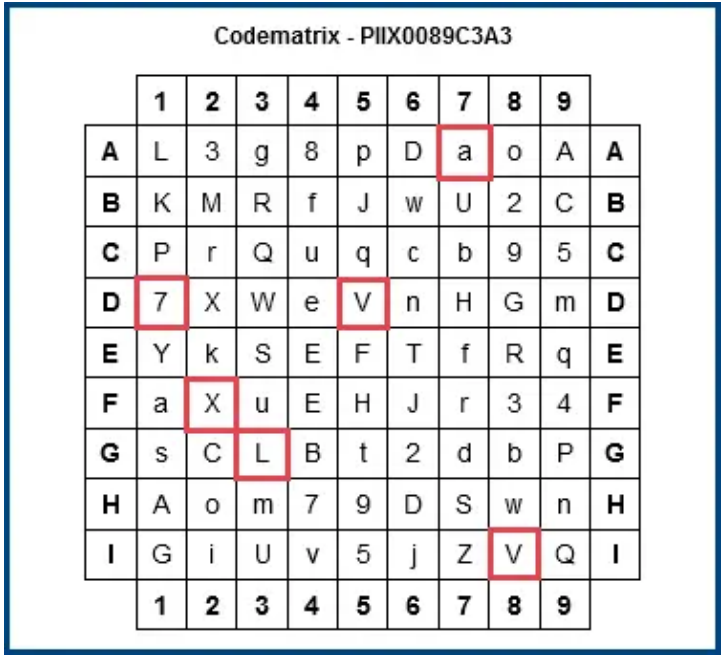
Geplanter Ablauf Rollout (Passkey + E-Mail)

- IT-Personal der zentralen IT
- Erster Flächentest in einem Bereich
- Zentralverwaltung
- Bedienstete der Lehre / Mitwirkende
- Studierende eventuell fakultätsweise / neu immatrikulierte Studierende und neue Bedienstet bereits bei Accountvergabe?

Rollout Passkeys

Schritte Umstellung

1. Rollout Codematrix mit bestehenden Credentials als Backuptoken (IAM-Portal über eduMFA-API)
2. Passkey über eduMFA-Portal, Login per Shibboleth mit Codematrix



	1	2	3	4	5	6	7	8	9	
A	L	3	g	8	p	D	a	o	A	A
B	K	M	R	f	J	w	U	2	C	B
C	P	r	Q	u	q	c	b	9	5	C
D	7	X	W	e	V	n	H	G	m	D
E	Y	k	S	E	F	T	f	R	q	E
F	a	X	u	E	H	J	r	3	4	F
G	s	C	L	B	t	2	d	b	P	G
H	A	o	m	7	9	D	S	w	n	H
I	G	i	U	v	5	j	Z	V	Q	I
	1	2	3	4	5	6	7	8	9	

Erfahrungen IT-Personal / Flächentest

- Anleitungen sind wichtig! Bringe Techniker zum Lesen, dann sind es 10 Minuten, sonst 60 ☺
- Multiplikatoren identifizieren
- individueller Unterstützungsbedarf für Nutzergruppen mit wenig IT-Erfahrung
- Zusätzlicher Registrationcode (nur einer 30 Minuten gültig) für Rollout Passkey per IAM-Portal, da Nutzerrückmeldung Codematrix zu schwierig zu handhaben
- Empfehlung 2. Device mit Passkey

Erfahrungen IT-Personal / Flächentest

- Linux Desktops keinen Support für Passkey mit TPM
- Windows 10 LTSC kein Passkey
- Teilweise veraltete TPM / Hardware nicht Windows 11
- Ausnahmen mfa-config.xml vornehmen
  - Electron Win10 LTSC, Electron Linux / Macos, Aktivierung Office keine Passkeyunterstützung
  - MFA in PC-Pools ➔ MFA generell nicht aktiv, nur für bestimmte Dienste erforderlich (Zugang zu PC-Pools wird als ausrechender Faktor angesehen für meiste Anwendungen)
- ggf. Push-App?

Zukunft Vergabe von Credentials / Token

1. Aktivierung Nutzerkonto
    1. per Aufgabe an private E-Mail-Adresse
    2. Vergabe Kennwort
    3. Rollout Codematrix
2. Passkey über eduMFA-Portal, Login per Shibboleth mit Codematrix bzw. Registrationcode, ggf. Push-App, Empfehlung 2. Device mit Passkey

Todos

- Anpassung Password-Workflows (z.B. PW-Reset nach Login mit Passkey ok, wenn Passkey defekt bootstrapping über IT-Support)
- Flächendeckender Rollout
- Abschaltung von LDAP bei allen Webanwendungen Ersatz Shibboleth (SAML / OIDC)
- Termial-Server evl. MFA mit Apache Guacamole

Fragen und Anregungen