

## HRZ



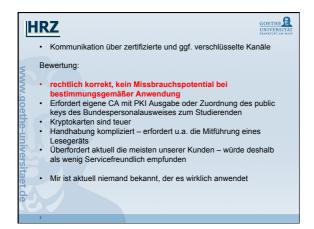
Richtige Beantwortung einer/mehrerer vorher hinterlegter Fragen (challenge-response) – Zusendung des neuen Passwords bei e-mail oder SMS

 Bewertung:
 Antworten dürfen nicht trivial zu erraten sein, oder sich aus persönlichen Gegenständen nicht leicht erschließen lassen – z.b. Gebursdatum oder Wohnadresse – solche Angaben können sich missliebige KommilitonInnen oder Taschendiebe leicht verschaffen. Überprüfung der Qualität der Fragen bei Hinterlegung?

Missbrauchspotential: Gering bis Mittel, abhängig von Anzahl und Qualität der Fragen
Hinreichender? Check der Identität wird so erreicht. Bei e-mail

Versandt erfolgt weiterhin eine nicht verschlüsselte Übertragung

2







_		
		OETHE R
	Bewertung: aus meiner Sicht sicher, uns ist bislang keine	NEFURT AM MAIN
	Schwachstelle des Verfahrens aufgefallen	
2	<ul> <li>App kann mit einer unabhörbaren PIN gesichert werden – Schi bei Diebstahl – sollte m.E. Pflicht werden.</li> </ul>	nutz
W.O	Kein Angriffspunkt durch key-logger etc. auf einem nicht	
oe:	vertrauenswürdigen Rechner.  • Keine zusätzlichen Werkzeuge notwendig, die der Nutzer nicht	nt
Πe	sowieso bei sich hat.	
	Vorteil: Verfahren erscheint "trendy", hohe Akzeptanz zu erwarten	n.
vers	Nachteil: Verbreitung von entsprechenden Handys erst bei 15 %,	
SILa	Tendenz aber stark steigend.  Direkte Nutzung ist auf Web-Services beschränkt, aber eine	
et.o	"neues Password"-Seite ist trivial möglich.	
9		
	10	
	IHRZ GO	OETHE A
	UN	NIVERSITAT
	Weitere Infos zum eKaay Verfahren	
5	www.ekaay.com	
<b>&gt;</b>		
0	Bernd Borchert WSI Uni Tübingen	

borchert@informatik.uni-tuebingen.de

Aktuell auf der Cebit am Gemeinschaftsstand des BMWi