Anwendung des "Technology Acceptance Model" zur Akzeptanzbestimmung qualifizierter elektronischer Fernsignaturen im Unternehmensumfeld

---

Interdisziplinäre und sozialwissenschaftliche Reflexion der Informatik 2

Wintersemester 2017/2018

Frank Dreyer
Matrikelnummer: 741827

07.02.2018

Inhaltsverzeichnis

1 Grundlagen

1.1 Technology Acceptance Model

Das *Technology Acceptance Model* [Dav85], kurz TAM, ist ein von von Fred D. Davis entwickeltes Akzeptanzmodell, welches auf dem sozialpsychologischem Modell *Theory of Reasond Action* (TRA) von Ajzen und Fishbein [AF80] basiert. Das Modell zielt darauf ab, Erkenntnisse darüber zu gewinnen, ob und warum Personen Technologien akzeptieren oder diese ablehnen.
Dabei wird angenommen, dass eine Person mit positiver Nutzungseinstellung zur Technologie diese auch tatsächlich verwendet. (Vgl. [BH09, p. 237]) Diese Nutzungseinstellung hängt wiederum maßgeblich von den Faktoren 'wahrgenommener Nutzen' und 'wahrgenommener Bedienungskomfort' ab.
Der 'wahrgenommene Nutzen' beschreibt das subjektiv Empfinden, dass sich eine Technologie positiv auf die Steigerung der eigenen Arbeitsleistung in einem organisatorischem Kontext auswirkt. (Vgl. [Dav89, p. 320])
Der 'wahrgenommene Bedienungskomfort' bezeichnet das subjektive Empfinden, dass die Verwendung einer Technologie mit wenig Aufwand verbunden ist, bzw. dass die Technologie einfach zu benutzen ist. (Vgl. [Dav89, p. 320])
Bandow und Holzmüller fassen die Auswirkung dieser beiden Determinanten folgendermaßen zusammen: "Je größer der Nutzen eines Informationssystems und je einfacher dessen Bedienbarkeit, desto eher ist der Anwender dazu bereit, das neue System zu nutzen." (Vgl. [BH09, p. 237])
Auf den 'wahrgenommenen Nutzen', wie auch den 'wahrgenommenen Bedienungskomfort' wirken wiederum 'externe Variablen', die unter anderem demografische und persönliche Merkmale des Akteurs umfassen, im Originalmodell allerdings nicht weiter spezifiziert werden. (Vgl. [Dav85, p. 21])
Abbildung 1 illustriert das Modell.

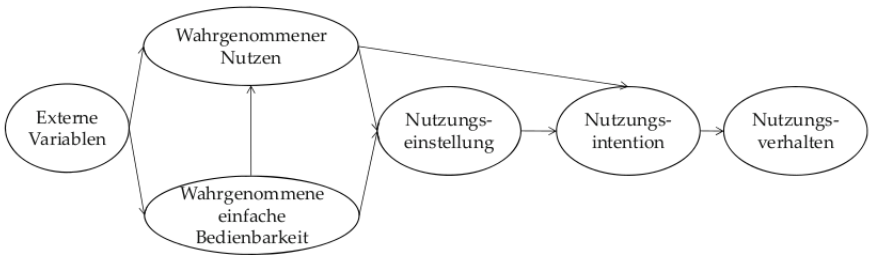

Abb. 1. *Technology Acceptance Model* (Vgl. [BH09, p. 237])

1.2 Digitale Signaturen

Digitale Signaturen sind in Grenzen vergleichbar mit konventionellen Unterschriften auf Papier, welche über ein asymmetrisches kryptographisches Ver-

fahren digitalisiert wurden. (Vgl. [PP16, p. 297]) Dieses asymmetrische Kryptosystem schließt drei Prozesse mit ein: den 'Unterschriftsprozess', den 'Authentifizierungsprozess' sowie den 'Prozess zur Sicherung der Datenintegrität'. (Vgl. [SDSLS15, p. 4])
Beim 'Unterschriftsprozess', muss sich die Person, die das jeweilige Dokument unterzeichnen soll, zunächst identifizieren. Die Identifikation hängt von der Implementierung ab und kann dementsprechend unter anderem über eine PIN, ein Passwort oder auch einen sequenz-basierten Token-Code abgewickelt werden. Ist die Identität des Unterzeichners bestätigt, so erhält er ein Zertifikat mit seiner Identität und einem öffentlichem und privatem Schlüsselpaar, mit dem er das Dokument signieren kann. Dafür wird zunächst ein einzigartiger mathematischer Code aus dem Dokument generiert, der im Anschluss über den privaten Schlüssel verschlüsselt, bzw. "signiert", wird. Um den 'Unterschriftsprozess' abzuschließen wird das Dokument zusammen mit der Signatur (dem verschlüsseltem mathematischen Code) an den Empfänger gesandt. (Vgl. [SDSLS15, p. 4])
Der Empfänger kann daraufhin im 'Authentifizierungsprozess' überprüfen, ob das Dokument auch von der richtigen Person unterzeichnet wurde. Dafür fordert er den öffentlichen Schlüssel der Unterzeichners an und kann daraufhin mit dem öffentlichen Schlüssel den mathematischen Code entschlüsseln. Das Entschlüsseln wird nur dann funktionieren, wenn das Dokument mit dem korrespondierenden privaten Schlüssel verschlüsselt wurde und kann daraus folgernd auch die Authentizität garantieren. (Vgl. [SDSLS15, p. 4])
Zum Schluss wird im 'Prozess zur Sicherung der Datenintegrität' überprüft, ob das Dokument nach dem Signieren nicht mehr verändert wurde. Dafür wird erneut der mathematische Code aus dem Dokument generiert und mit dem im 'Authentifizierungsprozess' entschlüsselten mathematischen Code verglichen. Beide müssen identisch sein um sicher zu sein, dass das Dokument nach dem Unterschreiben nicht modifiziert wurde. (Vgl. [SDSLS15, p. 4])

1.3 Qualifizierte Elektronische Signaturen

Von Qualifizierten Elektronischen Signaturen spricht man, wenn die Erzeugung einer digitalen Signatur dezentral über eine sichere Signaturerstellungseinheiten abgewickelt wird und die Signatur auf qualifizierten Zertifikaten beruht. (Vgl. [GWMK$^+$07, p. 8])
Die Signaturstellungseinheit, die auch Zertifizierungsstelle, Zertifizierungsdienstleister, *Certification Authority* (CA) oder auch *Public Key Infrastructure* (PKI) genannt wird, muss dabei vom Unterzeichner, als auch allen, die sich auf die Signatur verlassen oder berufen wollen, vertraut werden. (Vgl. [GWMK$^+$07, p. 9])
Darüber hinaus sind Zertifizierungsstellen, wie der Name bereits andeutet, für die Vergabe qualifizierter Zertifikate verantwortlich. Diese Zertifikate müssen bestimmte Angaben, wie z.B. den Namen des Inhabers, Angaben des Signaturschlüssels und den Gültigkeitszeitraum des Zertifikats enthalten. Außerdem müssen vor der Erstellung eines Zertifikats die Identität des zukünftigen Inhabers anhand von Ausweispapieren geprüft werden und der Zertifizierungsdienstleister

muss die Zertifikate über einen Zeitraum von mindestens fünf Jahren über offene Kommunikationskanäle für jedermann öffentlich zugänglich machen. (Vgl. [GWMK+07, p. 9])

1.4 Qualifizierte Elektronische Fernsignaturen

Von Qualifizieren Elektronischen Fernsignaturen spricht man, wenn bei einer Qualifizierten Elektronischen Signatur der private Schlüssel des Zertifikatinhabers bei der Signaturstellungseinheit liegt und von ihr verwaltet wird, wodurch der Signierer keine Smartcards, bzw. Speichermedien mit dem zugehörigen privaten Schlüssel, bei sich tragen muss. (Vgl. [Sch17, p. 30])

2 Der wahrgenommene Nutzen Qualifizierter Elektronischer Fernsignaturen

2.1 Effizienzsteigerung und Kostenminimierung dank schlanker Prozesse

Geschäftsabschlüsse, die durch eine handgeschriebene Unterschrift auf Papier durchgeführt werden, haben zwei entscheidende Nachteile: Sie verzögern die Wirtschaftlichkeit und steigern die Komplexität durch Archivierung.
Diese Nachteile können mit digitalen Signaturen, die über eine Zertifizierungsstelle durchgeführt und verwaltet werden, vermieden werden. Genehmigungen die bisher durch Prozesse wie Drucken, Versand, Scannen und Archivierung viel Zeit in Anspruch und Kosten durch Papier und Personal verursacht haben, können dadurch praktisch ohne Zeitverzögerung kostengünstig abgewickelt werden und sind Dank der Verwaltung durch die Signaturstellungseinheit leicht und jeder Zeit einsehbar.
Dieser Sachverhalt wird auch in einer von Arthur D. Little durchgeführten Befragung von 50 Marktexperten bestätigt. Sie schreiben: "Viele Unternehmen und Behörden haben bereits das Potential dieser Technologie erkannt. Ein vollständig digitaler Prozess für die Signierung und den Versand von Dokumenten senkt die Arbeitszeiten und Kosten für Papier und Transport." (Vgl. [SDSLS15, p. 7]) Darüber hinaus nennen die Teilnehmer der Befragung die Kosten- wie auch die Zeitersparnis als die zwei wichtigsten Vorteile beim Einsatz von Digitalen Signaturen. (Vgl. Abbildung [SDSLS15, p. 7]) Zwar könnte man argumentieren, dass Digitale Signaturen aufgrund der Implementierung hohe Kosten verursachen. Allerdings werden diese entstandenen Kosten schnell durch reduzierte Kosten aufgewogen. (Vgl. [SDSLS15, p. 7])

Literatur

[AF80] I. Ajzen and M. Fishbein, *Understanding Attitudes and Predicting Social Behavior*, Prentice Hall (1980).

[BH09] G. Bandow and H. Holzmüller, *"Das ist gar kein Modell!"*, Gabler Verlag, Wiesbaden, 2009.

[Dav85] F. Davis, *A technology acceptance model for empirically testing new end-user information systems - theory and results*, PhD Thesis, Massachusetts Inst. of Technology (1985).

[Dav89] ———, *Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*, MIS Quarterly (1989).

[GWMK+07] V. Gruhn, V. Wolf-Marting, A. Köhler, C. Haase, and T. Kresse, *Elektronische Signaturen in modernen Geschäftsprozessen*, Vieweg, Wiesbaden, 2007.

[PP16] C. Paar and J. Pelzl, *Kryptografie verständlich*, Springer Verlag, Berlin Heidelberg, 2016.

[Sch17] K. Schmeh, *Neue Signatur-Gesetzgebung: Sind aller guten Dinge drei?*, Springer Fachmedien (2017).

[SDSLS15] N. Schaettgen, J. Duvaud-Schelnast, D. Levy, and S. Socol, *Digitale Signaturen - Auf dem Weg zu einem digitalen Europa*, Arthur D. Little (2015).