

State-of-the-Art-Bericht zu elektronischen Daten- und Dokumentensafes

Universität Zürich
Arbeitsgruppe Informationsmanagement
Prof. Gerhard Schwabe

Erarbeitet von Joachim Pfister

Stand: Mai 2012

Inhalt

1	Einleitung und Aufbau	1
2	Persönliche Daten und Privacy.....	3
2.1	Persönliche Daten	3
2.1.1	Arten persönlicher Daten	3
2.1.2	Ökosystem persönlicher Daten	4
2.1.3	Persönliches Informationsmanagement und der Wert von Daten	6
2.2	Das Recht auf Privacy	9
2.3	User-managed Access zur informationellen Selbstbestimmung.....	10
2.3.1	Grundlagen.....	10
2.3.2	Anforderungen	12
2.3.3	Initiativen und Projekt.....	13
2.3.3.1	Zurück in die Zukunft: Von Infomediaries zum Vendor Relationship Management.....	13
2.3.3.2	Kantara initiative und User Managed Access	14
2.3.3.3	Information Card Initiative	16
2.3.3.4	Higgins	17
3	Technologien zur Durchsetzung von Privacy und User-managed Access.....	18
3.1	Elektronisches Identitätsmanagement	19
3.1.1	Authentifizierungsverfahren	20
3.1.2	Anonymität und Pseudonyme im eID-Kontext.....	22
3.2	Ländervergleich von eID-Lösungen	23
3.2.1	Österreich (aus Kubicek und Noack (2010))	26
3.2.2	Deutschland (aus Kubicek und Noack (2010)).....	27
3.2.3	Dänemark (aus Kubicek und Noack (2010))	27
3.2.4	SuisselD	28
3.2.5	Rundum-Erneuerung der Schweizer Identitätskarte und des Schweizer Passes	29
3.3	Elektronische Signatur	29
3.4	Akzeptanz von Sicherheitsmassnahmen	30
3.5	Bestehende EU-Projekte	32
3.5.1	ABC4Trust.....	32
4	Elektronische Datensafes.....	34
4.1	Vision und Terminologie	35

4.2	Nutzen.....	37
4.2.1	Safeanbieter	38
4.2.2	Safeinhaber	38
4.2.3	Dienstanbieter.....	38
4.2.3.1	Allgemeiner Nutzen für Dienstanbieter.....	39
4.2.3.2	E-Government-Dienstanbieter	39
4.2.3.3	Privatwirtschaftliche Dienstanbieter	39
4.3	Rechtliche Aspekte.....	40
4.3.1	Allgemeine rechtliche Aspekte.....	40
4.3.2	Problembereich der Zugriffsmöglichkeit staatlicher Stellen	41
4.3.3	Problembereich (eindeutige) Zustellung.....	41
4.4	Funktionen eines Datensafes.....	42
4.5	Anforderungen an einen Datensafebetreiber.....	44
4.6	Elektronische Datensafes in the Cloud.....	44
4.7	Dienste auf Basis elektronischer Datensafes	46
4.8	Vertrauenswürdige Digitalisierungsdienste als Hilfsdienst	48
4.9	Preismodelle für Datensafes	48
4.10	Interoperabilität und organisationsübergreifende Prozesse	49
4.11	Marktübersicht	53
4.11.1	Existierende Marktübersicht für den Finanzbereich	53
4.11.2	Existierende Marktübersicht zu Online-Storage-Anbietern	54
4.11.3	Elektronische Datensafes mit E-Government als vorwiegendem Treiber	54
4.11.4	E-Billing Consolidators.....	54
4.11.5	Elektronische Datensafes und Inventarisierungsdienste.....	55
4.11.6	Personal Data Stores mit Schwerpunkt VRM	55
5	Verwandte Bereiche	56
5.1	Elektronische Patientenakte	56
5.2	Elektronische Dokumentenzustellung	57
5.2.1	Allgemeines zu digitalen Postdiensten.....	57
5.2.2	De-Mail	58
5.2.3	Elektronisches Gerichts- und Verwaltungspostfach in Deutschland	60
5.2.4	Elektronischer Rechtsverkehr mit Behörden in der Schweiz.....	60
5.2.5	Inca-Mail.....	61
5.3	Elektronischer Rechnungsaustausch.....	61
5.3.1	Begriffsdefinition.....	61
5.3.2	Potentiale der elektronischen Rechnung	62
5.3.3	Verbreitung und Akzeptanz.....	63

5.3.4	Rechtliche Rahmenbedingungen in der Schweiz	66
5.3.5	Standards	67
5.3.6	Akteure bei der Erstellung von elektronischen Rechnungen	67
5.3.7	Anbieter von e-Invoicing Lösungen in der Schweiz	69
6	Portraits elektronische Dokumentensafes mit E-Government als vorwiegendem Treiber	70
6.1	Service-BW (Deutschland)	71
6.1.1	Kurzbeschreibung	71
6.1.2	Hintergrund zur Entstehung von „mein Service-BW“	71
6.1.3	Projektpartner	72
6.1.4	Finanzierung	72
6.1.5	Nutzung	72
6.1.5.1	Nutzerzahlen zum Datensafe	72
6.1.5.2	Nutzerzahlen des Service-BW-Portals	72
6.1.5.3	Nutzung der Online-Fachverfahren	72
6.1.6	Verhältnis zu De-Mail bzw. De-Safe	72
6.1.7	Funktionen	73
6.1.7.1	Datenverschlüsselung und Datenschutz	73
6.1.7.2	Zugang	73
6.1.7.3	Recovery-Mechanismen	73
6.1.7.4	Freigabe von Dokumenten	73
6.1.7.5	Freigabe an einen Workflow	74
6.1.7.6	Freigabe von Einzeldaten	74
6.1.7.7	Suche über die Dokumente	74
6.1.7.8	Was geschieht mit den Daten nach dem Tod des Nutzers?	74
6.1.8	Was hat man noch nicht erreicht?	74
6.1.9	Zukünftige Entwicklungen	74
6.1.10	Besonderheiten „mein Service-BW“	74
6.2	De-Safe (Deutschland)	76
6.2.1	Kurzbeschreibung	76
6.2.2	Hintergrund zur Dokumentenablage bei De-Mail (De-Safe)	76
6.2.3	Projektpartner	76
6.2.4	Finanzierung und Geschäftsmodell	76
6.2.5	Nutzung und Testbetrieb	78
6.2.6	Funktionen	78
6.2.6.1	Datenverschlüsselung und Datenschutz	78
6.2.6.2	Zugang	78
6.2.6.3	Recovery-Mechanismen	78
6.2.6.4	Upload von Dokumenten	78
6.2.6.5	Standard Dokument- und Verzeichnis-Operationen	78
6.2.6.6	Kategorien als Ordnungsmittel	79
6.2.6.7	Freigabe von Dokumenten	79
6.2.6.8	Suchfunktion	79
6.2.6.9	Protokollierung	79
6.2.6.10	Was geschieht mit den Daten nach dem Tod des Nutzers?	79
6.2.7	Rechtliche Aspekte der Zustellung	79
6.2.8	Besonderheiten zum DE-Safe	80

6.3	Governikus eBürgersafe (Deutschland)	81
6.3.1	Kurzbeschreibung	81
6.3.2	Hintergrund zur Entstehung des eBürgersafes	81
6.3.3	Projektpartner	81
6.3.3.1	Hersteller	81
6.3.3.2	Produktanwender	81
6.3.4	Finanzierung	81
6.3.5	Geschäftsmodell	81
6.3.6	Nutzung	82
6.3.6.1	Nutzerzahlen	82
6.3.6.2	Datenvolumen	82
6.3.7	Verhältnis zu De-Mail bzw. DE-Safe	82
6.3.8	Funktionen	82
6.3.8.1	Datenverschlüsselung und Datenschutz	82
6.3.8.2	Zugang	82
6.3.8.3	Recovery-Mechanismen	82
6.3.8.4	Nur einfache Funktionen werden angeboten	82
6.3.8.5	Was geschieht mit den Daten nach dem Tod des Nutzers?	83
6.3.9	Zukünftige Entwicklungen	83
6.3.10	Einbindung von Datenschützern	83
6.3.11	Besonderheiten zum eBürgersafe	83
6.4	doMap (Deutschland)	84
6.4.1	Kurzbeschreibung	84
6.4.2	Hintergrund zur Entstehung von doMap	84
6.4.3	Projektpartner	84
6.4.4	Finanzierung	85
6.4.5	Geschäftsmodell	85
6.4.6	Architektur	85
6.4.7	Nutzung	87
6.4.7.1	Nutzerzahlen und Nutzungshäufigkeit	87
6.4.7.2	Nutzerzufriedenheit	87
6.4.8	Funktionen	88
6.4.8.1	Datenverschlüsselung und Datenschutz	88
6.4.8.2	Zugang	88
6.4.8.3	Recovery-Mechanismen	89
6.4.8.4	Gibt es eine Übersicht für den Bürger, welche Daten er alle weitergegeben hat?	89
6.4.8.5	Benachrichtigungen über den Bearbeitungsstand	89
6.4.8.6	Freigabe von Daten / Dokumentensafe	89
6.4.8.7	Delegation	89
6.4.8.8	Protokollfunktion	89
6.4.8.9	Was geschieht mit den Daten nach dem Tod des Nutzers?	90
6.4.8.10	Abwicklung verwaltungsinterner Geschäftsprozesse	90
6.4.8.11	Behördenübergreifende Geschäftsprozesse	90
6.4.8.12	Qualifizierte elektronische Signatur	90
6.4.9	Zukünftige Verbindung von doMap mit De-Mail bzw. DE-Safe?	90
6.4.10	Prozessunterstützung	90
6.4.10.1	Entscheidung, welche Prozesse digital umgesetzt werden	90
6.4.10.2	Vorgehen zur Umsetzung neuer Prozesse	91
6.4.11	Zukünftige Entwicklungen	91

6.4.11.1	Verbreiten der Lösung und Entwicklungspartnerschaften	91
6.4.11.2	Verfahren zur Bürgerbeteiligung	91
6.4.11.3	Authentisierung über den neuen (deutschen) Personalausweis	91
6.4.12	Stolpersteine	91
6.4.13	Besonderheiten bei doMap	91
6.5	e-Boks (Dänemark)	93
6.5.1	Kurzbeschreibung	93
6.5.2	Hintergrund zur Entstehung von e-Boks	93
6.5.3	Betreiber	93
6.5.4	Finanzierung und Geschäftsmodell	93
6.5.5	Nutzung und Nutzerzufriedenheit	93
6.5.5.1	Nutzung durch die Endnutzer	93
6.5.5.2	Nutzung auf Anbieterseite	94
6.5.5.3	Beurteilung der Nutzerfreundlichkeit durch die Endanwender	94
6.5.5.4	Anzahl versandter Dokumente	94
6.5.5.5	Angaben zum Bekanntheitsgrad	94
6.5.6	Funktionen	94
6.5.6.1	Datenverschlüsselung und Datenschutz	94
6.5.6.2	Zugang	94
6.5.6.3	Recovery-Mechanismen	95
6.5.6.4	Freigabe von Dokumenten	95
6.5.6.5	Freigabe von Einzeldaten	95
6.5.6.6	Ordner	95
6.5.6.7	Benachrichtigung (E-Mail) über neue Inhalte	95
6.5.6.8	Benachrichtigung (SMS) über ein separates Portal	95
6.5.6.9	Was geschieht mit den Daten nach dem Tod des Nutzers?	95
6.5.6.10	Auswahl der akzeptierten Versender	95
6.5.6.11	Hochladen von eigenen Dokumenten	95
6.5.6.12	Nachrichtenaustausch	95
6.5.7	Zukünftige Entwicklung	97
6.5.8	Besonderheiten bei e-Boks	97
6.5.9	Nutzerstimmen	97
6.6	E-Tresor (Österreich)	98
6.6.1	Kurzbeschreibung	98
6.6.2	Hintergrund zur Entstehung des E-Tresors	98
6.6.3	Betreiber	98
6.6.4	Finanzierung und Geschäftsmodell	98
6.6.5	Nutzung	99
6.6.6	Zielsetzung	99
6.6.7	Funktionen	99
6.6.7.1	Datenverschlüsselung und Datenschutz	99
6.6.7.2	Zugang	100
6.6.7.3	Recovery-Mechanismen	100
6.6.7.4	Upload von Dokumenten	100
6.6.7.5	Freigabe von Dokumenten	101
6.6.7.6	Ordner	102
6.6.7.7	Benachrichtigung über neue Inhalte bzw. erhaltene Freigaben	102
6.6.7.8	Was geschieht mit den Daten nach dem Tod des Nutzers?	102
6.6.7.9	Passwortsafe	103
6.6.7.10	Protokollfunktion	103

6.6.7.11	Erinnerungsfunktion	103
6.6.7.12	Elektronisches Signieren von Dokumenten	104
6.6.7.13	Verwaltungsfunktionen	105
6.6.8	Besonderheiten beim E-Tresor	106
6.6.9	Weitere Lösungen	107
6.7	Übersicht über elektronische Dokumentensafes mit E-Government als vorwiegendem Treiber	108

7 E-Billing Consolidators 109

7.1	Adminium	109
7.1.1	Kurzbeschreibung	109
7.1.2	Betreiber	109
7.1.3	Finanzierung und Geschäftsmodell	109
7.1.4	Angaben zur aktuellen Nutzung	109
7.1.5	Angaben zu den einzelnen Funktionen	109
7.1.5.1	Datenverschlüsselung und Datenschutz	109
7.1.5.2	Zugang (Login)	109
7.1.5.3	Upload von Dokumenten	110
7.1.5.4	Empfang von Dokumenten von Anbietern	110
7.1.5.5	Benachrichtigungen	110
7.1.5.6	Freigabe von Dokumenten oder des Kontos	110
7.1.5.7	Ordner	110
7.1.5.8	Suche über Dokumente	110
7.1.5.9	Protokollierung	110
7.1.5.10	Was geschieht mit den Daten nach dem Tod des Nutzers?	110
7.1.6	Besonderheiten von Adminium	110
7.2	Vaultstreet.com	111
7.3	Zumbox	111
7.4	Doxo	112
7.5	Manilla	112
7.6	Volly	113
7.7	Übersicht über E-Billing Consolidators	115

8 Elektronische Datensafes und Inventarisierungsdienste 116

8.1	InformationSafe	116
8.2	Orggitt.com	117
8.3	Anwendungen zur Inventarisierung	117
8.3.1	Inventarisierung von Wohnungen	117
8.3.2	Inventarisierung von Wertgegenständen	118
8.3.3	Verbindung der Inventarisierungs-Anwendungen mit Cloud-Storage-Anbietern	119

9	Personal Data Stores mit Schwerpunkt VRM.....	120
9.1	Mydex (Vereinigtes Königreich)	120
9.1.1	Kurzbeschreibung	120
9.1.2	Projektpartner	120
9.1.3	Finanzierung und Geschäftsmodell	120
9.1.4	Beteiligung an anderen Initiativen	121
9.1.5	Funktionalitäten	121
9.1.5.1	Datenschutz und Datenverschlüsselung	121
9.1.5.2	Zugang	121
9.1.5.3	Recovery-Mechanismen	121
9.1.5.4	Freigabe von Datenattributen und Dokumenten	122
9.1.5.5	Was passiert, wenn der Nutzer stirbt?	122
9.1.6	Weitere Erkenntnisse	122
9.1.6.1	Erstellung eines eigenen Metadaten-Modells für den Data Store:	122
9.1.6.2	Vertrauensproblematik (Cloud-Storage):	122
9.1.6.3	Mydex-Prototyp	122
9.1.6.4	Haltung der öffentlichen Hand gegenüber Mydex	123
9.1.6.5	Wo lagen die grössten Probleme?	123
9.1.6.6	Was war leichter als gedacht?	123
9.1.7	Besonderheiten bei Mydex	123
9.2	Pidder	124
9.2.1	Kurzbeschreibung	124
9.2.2	Betreiber	124
9.2.3	Geschäftsmodell	125
9.2.4	Angaben zur aktuellen Nutzung	125
9.2.5	Angaben zu den einzelnen Funktionen	125
9.2.5.1	Datenverschlüsselung und Datenschutz	125
9.2.5.2	Zugang	125
9.2.5.3	Recovery-Mechanismen	126
9.2.5.4	Freigabe von Einzeldaten	126
9.2.6	Nachrichtenaustausch	126
9.2.7	Besonderheiten von pidder	127
9.3	Personal	127
9.4	Azigo	129
9.5	TrustFabric	130
9.6	Allow	132
9.7	Singly	132
9.8	Qiy	132
9.9	Übersicht über Personal Data Stores mit Schwerpunkt VRM	134
10	Vergleich der Geschäftsmodelle elektronischer Datensafes	135

11	Implikationen für die Data Purse	149
11.1	Wirtschaftliche Herausforderungen	149
11.2	Technische Herausforderungen	150
11.3	Rechtliche Herausforderungen	151
11.4	Herausforderungen aus Nutzersicht	152
11.5	Stakeholder im geplanten Data Purse-Projekt	153
12	Literaturverzeichnis	155
Anhang A	Fragebögen	A-1
Anhang A.1	Mein Service-BW	A-1
Anhang A.2	eBürgersafe	A-4
Anhang A.3	Mydex	A-7
Anhang A.4	doMap	A-10
Anhang A.5	A-13
Anhang A.6	De-Safe	A-15
Anhang A.7	e-Boks Endanwender	A-17
Anhang B	Verwaltungsinterner Workflow bei doMap	B-1
Anhang C	Auftragsabwicklung für Sachbearbeiter bei doMap	C-1