Report der Gruppe 2, Version 1.4, 22.Mai 2010, 12.45

Moderator: Reinhard Riedl
Rapporteur: Olivier Glassey
Responsible Authors: Reinhard Riedl, Olivier Glassey;

Teilnehmer Tag 1 (Durchführung einer SWOT Analyse): Willy Müller, Stefan Walser, Thomas Brenikofer, Ka Schuppisser, Alberto Bondolfi, Reinhard Anton, Urs Bürge, Urs Gröhbiel, Olivier Glassey, David Rosenthal, Reinhard Riedl, Marc Zweiacker;

Teilnehmer Tag 2 (Identifikation von Empfehlungen und Aktion, Clustering der Empfehlungen zu Handlungsfeldern, Priorisierung der Aktionen): Willy Müller, Stefan Walser, Thomas Brenzikofer, Ka Schuppisser, Olivier Glassey, David Rosenthal, Reinhard Riedl, Marc Zweiacker, Peter Fischer, Urs Gröhbiel, Reinhard Anton;

Beobachtung – Es gibt ein Window of Opportunity

Vertrauen ist eine Grundvoraussetzung für jede Form von erfolgreichem wirtschaftlichen Handeln und von gutem sozialem Zusammenleben. Mit der SuisseID öffnet sich ein „Window of Opportunity“ zur Weiterentwicklung der vertrauenswürdiger Kommunikation und Interaktion über das Internet. Dies ist für die zukünftige Entwicklung der Schweiz von kritischer Bedeutung, weil ein wesentlicher Teil der Entwicklung auf internetbasierter Kommunikation basieren wird, welche Vertrauenswürdigkeit besitzen und Vertrauen gewinn muss.

Das Window of Opportunity existiert aus drei Gründen: Erstens sind sehr viele Kontextfaktoren günstig. Die Technologie existiert. Ein grosses Grundvertrauen ist vorhanden. Die institutionelle Sicherheit und die politische Stabilität sind hoch, der Bildungsstand der Bevölkerung ist hoch und die Nutzung von Informations- und Kommunikationstechnologie ist sehr weit verbreitet – bei Jugendlich sogar annähernd zu 100%. Zweitens steht mit der SuisseID eine einfache Lösung mit praktisch unbeschränkter Skalierbarkeit zur Verfügung, die universell einsetzbar ist. Drittens wird die SuisseID nicht nur vom Bundesrat und von vielen Akteuren gepuscht, sondern es ist auch die Bereitschaft der Wirtschaft sehr hoch, die SuisseID zu nutzen und selber zu puschen.

Wird das Window of Opportunity genutzt, könnte die Schweiz europaweit sogar zur führenden Nation im Bereich eSociety und eEconomy werden. Es gibt aber verschiedenste Gefahren, die dazu fügren könnten, dass sich das Window of Opportunity schliesst bevor es genutzt werden kann – in welchem Fall die SuissID eventuell sogar zu einer Blockade für die Entwicklung von eEconomy und eSociety für einige Jahre werden könnte. Daraus leitet sich die Frage ab, was getan werden kann, damit das Window of Opportunity genutzt werden kann.

Empfehlung 1: Governance durch partizipativ entwickelte Standards

Wir empfehlen eine Governance durch Standards, die von Privatwirtschaft und Behörden gemeinsam entwickelt werden. Standards sind strategisch als Führungsinstrument wichtig, weil sie eine gemeinsame Orientierung der Akteure ermöglichen. Sie sind operativ wichtig, weil sie Interoperabilität, d.h. eine zugleich freie und sichere Interaktion über Organisationsgrenzen hinweg, ermöglichen. Wobei erst die operativen Qualitäten die strategischen Qualitäten wirksam werden lassen. Die partizipative Entwicklung von Standards wiederum ist in dreierlei Hinsicht von Nutzen: Sie ermöglicht eine breite Nutzung des vorhandenen Wissens. Sie schafft eine geteilte Ownership,

die eine Verbreitung auf unterschiedlichen Kanälen ermöglicht. Und einer Ablehnung eines Standards als fremder Fötzel wird die moralische Rechtfertigung genommen.

Aktion 1.1
Der SuisseID-Standard sollte gepflegt und auf der Basis der gemachten Erfahrungen weiterentwickekt werden – möglichst durch einen breit abgestützten Trägerverein. (Diese Aktivität ist bereits geplant.) Diese Aktion hat erste Priorität!

Empfehlung 2: Internationale Interoperabilität

Wir empfehlen eine sichere Öffnung der Schweizer eEconomy und eSociety, indem die sichere Anwendbarkeit der SuisseID im Ausland und die sichere Nutzung ausländischer elektronischer Identitäten in der Schweiz sollte ermöglicht werden. Dies ist ein Fall, wo der Foifer unds Weggli möglich sind: Die proaktiven Beschränkungen werden aufgehoben und trotzdem wird die reale Sicherheit erhöht, weil die Interoperabilität zhwischen sicheren Systemen im Inland und sicheren Systemen im Ausland im Missbrauchsfall eine bessre reaktive Identifikation von Tätern und Verantwortlichen ermöglicht.

Aktion 2.1
Die Interoperabilität mit den STORK-Standards sollte hergestellt werden. STORK zielt darauf ab, europaweite Interoperabilität sehr unterschiedlicher Lösungen im Kontext von digitaler Identität zu vernetzen. Es ist deshalb die erste Wahl für die Implementierung der Interoperabilität zwischen Schweiz und Europa.

Empfehlung 3 – Die rechtlichen Rahmenbedingungen vertrauenswürdiger machen

Wir empfehlen die Quellen von Misstrauen im Schweizer Rechtssystem systematisch trocken zu legen. Bürger und KMUs sollen Vertrauen fassen, dass der Staat Fairness garanmtiert bei der Verteilungen der Risiken der digitalen Kommunikation in der eSociety und der eEconomy. Dieses Vertrauen wird die Bereitschaft erhöhen, die SuisseID aktiv zu nutzen. Weiters empfehlen, die Einsetzbarkeit vertrauendwürdiger Instrumente wie der SuisseID im öffentlichen Recht abzustützen.

Aktion 3.1a
Die Möglichkeiten von Firmen, die Risiken der Nutzung von Internetkommunikation einseitig auf die Kunden abzuwenden sollen rechtlich eingeschränkt werden. Diese Aktion hat erste Priorität!

Aktion 3.1b
Die im Gesetz festgelegten Risiken der Bürger bei der Nutzung von Instrumenten wie der SuissID sollen eingeschränkt werden.

Aktion 3.2
Präzedenzfälle sollen durch den Datenschzutbeauftragten geschaffen werden, die zeigen, dass sich Bürger gegen Verletzung des Datenschutzes erfolgreich wehren können. Diese Massnahme ist a priori ambivalent, weil sie das Vertrauen in den Schutz durch den Staat stärkt, aber eventuell auch abschreckt, überhaupt das Internet aktiv zu nutzen. Die abschreckende Wirkung auf Unternehmen mit Missbrauchsabsichten wird aber die Sicherheit erhöhen, also die objektiven Voraussetzungen für Vertrauen verbessern.

Aktion 3.3
Der Wissenstand der Akteure in der Justiz in Bezug auf die IKT, ihre Möglichkeiten und ihre

Risiken sollte durch Weiterbildung und Informationsportale verbessert werden. Im Bereich der Weiterbildung sollten neben konkreten Hochschulangeboten insbesondere auch Wissensaustauschplattformen entstehen. Dafür als Beispiel dienen kann unter anderen die Salzburger IRIS.

Aktion 3.4
Im öffentlichen Recht sollten die Voraussetzungen für einen breiten Einsatz der SuisseID im E-Government geschaffen werden.

Empfehlung 4 – Die öffentliche Debatte starten: Awareness and Wisdom of the Crowd

Wir empfehlen, eine breite Debatte über die Governance des Internet zu starten, um zugleich das Wissen über Risiken und Gefahren zu verbreiten und partiziptativ zu Governance-Lösungen zu kommen, die auf dem Wissen und den Erfahrungen der vielen, das heisst der Masse der Internetnutzer beruhen. Diese öffentliche Debatte sollte von Regierungen, Parteien und Interessensorganisationen durch Wahrnehmung und Feedback gefördert werden.

Aktion 4.1
Eine Internetlandsgemeinde Schweizer Jugendlicher, bzw. von Jugendlichen in der Schweiz, sollte einberufen werden, um die Herausforderungen für die Internet-Governance zu besprechen und gemeinsam Lösungsvorschläge zu diskutieren, bzw. in kleinen Gruppen neue Lösungsvorschläge zu erarbeiten. Diese Internetlandsgemeinde sollte sich vorzugsweise sowohl physisch als auch virtuell treffen. Wichtig ist, dass die Ergebnisse in den Parlamenten und von den Schweizer ICAN Vertretern diskutiert werden, um den Teilnehmern der Landsgemeinde das Gefühl zu vermitteln, das ihre Tätigkeit ernst genommen wird und etwas bewirken kann.

Empfehlung 5 – Von schnellen Erfolgen zur Nachhaltigkeit

Um das Window of Opportunity zu nutzen, müssen erstens schnelle Erfolge erzielt, zweitens diese Erfolge breit und effektiv kommuniziert und drittens die Erfolge durch eine Organisationsinfrastruktur abgestützt werden. Wir empfehlen deshalb, auf breiter Basis die schnelle Implementierung von Vorzeigebeispielen zu fördern und diese möglichst breit zu kommunizieren. Diese Vorzeigebeispiele sollten zu einer Kampagne für den breiten Einsatz der SuisseID genutzt werden. Wichtig ist, neben dem Nutzen auch die einfache Machbarkeit aufzuzeigen und einen SuissID-Groove zu erzeugen. Um die Nachhaltigkeit sicherzustellen, empfehlen wir den Aufbau eines Informationsintermediär für Identitätsmanagement-Informationen zu etablieren. Dieser soll eine sicheres Upscaling des Systems entstehender Dienste ermöglichen. Wichtig wäreweiters, dass die Bundesregierunng und die Kantonsregierungen ihr Commitmment zum Thema SuisseID im Speziellen und zur Weiterentwicklung von eSociety und eEconomy geben.

Aktion 5.1
Im Bereich des Funktionsnachweises der SuisseID sollten möglichst schnell schweizweite Dienste implementiert werden. Für diese Implementierung sollte eine PR-Kampagne gestartet werden. Diese Aktion hat erste Priorität.

Aktion 5.2
Es soll eine breite PR-Kampagne gestartet werden, mit dem Ziel, dass jede Schweizer G2B oder G2C E-Government Anwendung mit Transaktionsmöglichkeiten SuisseID-enabled wird.

Aktion 5.3

Es soll ein Informationsintermediär etabliert werden, der eine zur SIX-Telekurs im Bankensektor analoge Rolle im Bereich des Indentitätsmanagements hat.

Aktion 5.4
Eine Forschungsidentität sollte geschaffen und mit Kollaborationsumgebungen an Hochschulen und an öffentlichen und privaten Forschungsinstituten verknüpft werden, um eine möglichst uneingeschränkte Zusammenarbeit in der Forschung über Organisationsgrenzen zu unterstützen.

Aktion 5.5
Eine Bildungsidentität soll geschaffen werden, die lebenslang von Kindergarten bis zur Seniorenweiterbildung genutzt werden kann – möglichst auch Ausbildungen im Ausland, beispielsweise bei Auslandssemestern. Letzteres würde durch die Schaffung von Interoperabilität mit den STORK-Standards möglich (vergleiche Aktion 2.1).

Aktion 5.56
Die Bundesregierung sollte ein langfristiges Committment zum Ausbau der IT-Infrastruktur für eSociety und eEconomy geben.

Empfehlung 6: Wissen schafft Kompetenzen – Kompetenzen schaffen Sicherheit – Sicherheit schafft Vertrauen

Das Wissen in der Bevölkerung ist sowohl in Bezug auf die Gefahren des Identitätsmissbrauchs in der eSociety und eEconomy, als auch in Bezug auf pragmatische Möglichkeiten für effektives Risikomanagement gering. Oft wird gleichzeitig in einigen Bereichen hundertprozentige Sicherheit angestrebt und in anderen Bereichen die Sicherheit vernachlässigt. Das heisst, es fehlen insbesondere die Kompetenzen für ein pragmatisches Risikomanagement, das sich am erwartbaren Schaden ausrichtet. Ungefährliche Nutzungen des Internet werden ebenso ängstlich vermieden wie echte, schwerwiegende Gefahren von den gleichen Menschen verdrängt werden. Sinnvoller wäre stattdessen ein „ausgeglichener“, konkrete Gefahrenfolgen abwägender Umgang mit Risiken. Deshalb empfehlen wir, Wissen und Kompetenzen auf breiter Basis im Rahmen einer Kampagne zu vermitteln. Dies hilft nur nicht dem Einzelnen, sondern macht auch das system als ganzes sichrer, weil naives Verhalten von Einzelnen stets auch eine indirekte Gefahr für das System als ganzes darstellt. Wissen, Kompetenzen und die erhöhte Sicherheit als ganzes wird die Basis für ein kritisches – und deshalb nachhaltiges – Vertrauen schaffen.

Aktion 6.1
Einw breite Sensibilisierungskampagne soll durchgeführt werden, die sich an alle Stakeholder richtet – neben Bürgern und Beamten auch und insbesondere an KMUs. Im Rahmen dieser Kampagne soll nicht nur Bewusstsein, sondern es sollen auch Bewusstsein und Kompetenzen vermittelt werden. Diese Aktion hat erste Priorität!

Empfehlung 7: Veranstaltungszentren profitieren nachhaltig – Schweiz 3.0 als Zentrum der Informations- und Vertrauenssbroker

Orte, die als internationale Veranstaltungszentren fungieren, haben in der Vergangenheit von dieser Funktion stets sehr nachhaltig profitieren. Wer Exzellenz unterschiedlichster Provenienz anzieht, schafft einen Nährboden für die Exzellenz des eigenen Nachwuchses. Wir empfehlen deshalb, dass die Schweiz zu einem Zentrum für Veranstaltungen im Themenfeld virtuelle Identität wird. Langfristig könnte die Schweiz, die einst ein Zentrum des Kriegshandwerks war und heute ein Zentrum des Finanzwesens ist, in Zukunft ein Zentrum für Vertrauens- und Informationsintermediäre werden.

Aktion 7.1
Die Schweiz sollte gezielt zu einem Zentrum für Informationsaustauschevents zu virtueller Indentität und zu Vertrauensintermediären werden. Dies sollte durch eine Programmorganisation und ein Committment von Seiten Bundesrat und KdK unterstützt werden.

Aktion 7.2
Es sollten Bar-Camps zum Thema virtuelle Identität, soziale Medien und Internet-Governance durchgeführt werden.

Empfehlung 8: Versicherungen schaffen Vertrauen

Bisher gibt es kaum Möglichkeiten, sich gegen Schäden aus dem Missbrauch von Identitätsinformationen zu versichern. Identitätsmanagement ist in dieser Hinsicht ein singulären Risikobereich – was wesentlich zu einer Fokussierung auf präventive proaktive Massnahmen unter Ausschluss der Planung möglicher reaktiver Massnahmen beiträgt. Diese präventiven Massnahmen können aber nie hundertprozentige Sicherheit bieten und teils ist das Verhältnis von Sicherheit versus Kosten schlicht generalpräventic – entweder für die Ausübung von Geschäftstätigkeit oder (!) für die Schaffung persönlicher Sicherheit. Wir empfehlen deshalb, dass entsprechende Versicherungsprodukte angeboten werden und dass die für die Kreierung dieser Versicherungsprodukte notwendige Forschung in Zusammenarbeit mit den Schweizer Hochschulen durchgeführt wird.

Aktion 8.1
Versicherungsprodukte sollen in KTI-Projekten entwickelt werden.

Empfehlung 9: Keine Nachhaltigkeit ohne Forschung

Die Schweizer Praktiker und involvierten Institutionen haben in aller regel weniger Überblick über internationale Trends und Innovationen als die wenigen spezialisierten Forscher an Schweizer Hochschulen. Wir empfehlen deshalb, dass Hochschulen für WTT aus dem Ausland in die Schweiz sorgen. Weiter ist das Wissen über den Umgang mit der eigenen digitalen Identitäten, d.h. den eigenen digitalen Datenspuren, und das Wissen über das Realvertrauen in Internetkommunikation und seine Folgen ist gering. Grund ist, dass sich die Forschung in aller Regel entweder mit dem „politischen“ oder mit dem „Technischen“ beschäftigt, aber derzeit noch sehr selten mit dem „Technopolitischen“. Konkrete Forschungsprogramme zu virtueller Identität und Vertrauen aus technopolitischer, ganzheitlicher, multi- und transdisziplinärer Sicht fehlen derzeit. Wir empfehlen deshalb, entsprechende Forschung durchzuführen.

Aktion 9.1
Die Hochschulen sollten einen Monitoring internationaler Aktivitäten durchführen und mittels WTT-Veranstaltungen für einen Erfahrungsimport sorgen. Die Veranstaltungen sollten durch die Wirtschaft unterstützt werden.

Aktion 9.2
Die Erfolge der Schweiz sollten auch im Ausland in den entsprechenden Communities bekannt gemacht werden. Dies sollte durch eine Zusammenarbeit zwischen involvierten Praktikern und Hochschulen geschehen.

Aktion 9.3
Das Verhalten in Bezug auf die eigene digitale Identität sollte ganz grundsätzlich erforscht werden.

Empfehlung 10: Kein Vertrauen ohne Usability

Die Nutzung von Identitätsmanagement-Werkzeugen scheitert oft an der schwierigen Verständlichkeit und Bedienbarkeit dieser Werkzeuge. Wir empfehlen Usability als Qualitätsmerkmal viel stärker als bisher zu thematisieren.

Aktion 10.1
Guidelines für Usability von Identitätsmanagement-Werkzeugen sollten gemeinsam von Behörden, Wirtschaft und Hochschulen entwickelt. Dies gilt insbesondere für die Benutzerschnittstelle zur Eigendefinition der Zugreifbarkeit von identitätsbezogenen Daten in sozialen Medien, aber auch für Werkzeuge zur Verwaltung digitaler Identitäten in unterschiedlichen Kontexten.

Aktion 10.2
Eine Usability-Zertifizierung sollte sowohl für Identitätsmanagement-Werkzeuge angeboten werden.

Aktion 10.3
Werkzeuge sollten entwickelt werden, die es Nutzern ermöglichen, ihre digitale Identitäten kontrolliert und so weitgehend wie möglich zu löschen. Damit iist nicht das Löschen von Accounts gemeint, das in der Regel einfach ist, sondern das Löschen von Daten.