SATW Workshop Münchenwiler 20./21. Mai 2010
Ergebnisbericht der Gruppe 2 (DRAFT!) Version 2.0, 30. Juni 2010, 23.00

The Window of Opportunity Is Open
(1 Observation – 10 Recommendations – 36 Actions)

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

Teilnehmer (Gruppe 2): Reinhard Anton, Alberto Bondolfi, Urs Bürge, Thomas Brenzikofer, Peter Fischer, Olivier Glassey, Urs Gröhbiel, Willy Müller, Reinhard Riedl, David Rosenthal, Ka Schuppisser, Stefan Walser, Marc Zweiacker;

Programm:

- ☒ Tag 1(1 Sitzung): SWOT-Analyse
- ☒ Tag 2 (2 Sitzungen): Identifikation von Empfehlungen und Aktionen, Clustering der Empfehlungen zu Handlungsfeldern, Selektion und Priorisierung der empfohlenen Aktionen in den Handlungsfeldern

Disclaimer: Das Ergebnis ist eine textliche Ausarbeitung der Gruppenresultate, die auf bunten Zetteln und in einem Steckbild, sowie durch die Mitschrift von zwei Rapporteuren dokumentiert wurden. Der Text gibt einen Gruppenkonsens wieder und impliziert nicht, dass jeder Beteiligte allen Aussagen umfänglich zustimmt. Im Rahmen der Ausarbeitung wurden einige Ergänzungen in Bezug auf die Aktionen gemacht und einige neue Zuordnungen von Aktionen vorgenommen (insgesamt ca. 20%). Ausserdem wurden die Ergebnisse des Debriefings zum Workshop in der e-Society-Arbeitsgruppe der SATW berücksichtigt. Weitere kleine Änderungen erfolgten in einer feedbackrunde auf Vorschlag der Workshopteilnehmer.

Der Arbeitsprozess wurde so gestaltet, dass er zu ***Idea Richness*** führt. Ein kleinster gemeinsamer Nenner wurde nicht angestrebt!

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 Anfang Mai lancierten SuisseID öffnet sich ein ***„Window of Opportunity" zur Weiterentwicklung der vertrauenswürdiger Kommunikation und Interaktion über das Internet in der Schweiz***. Die Nutzung dieses Opportunitätsfensters ist für die zukünftige Entwicklung der Schweiz von kritischer Bedeutung, weil ein wesentlicher Teil der Entwicklung auf internetbasierter Kommunikation basieren wird. Und diese sollte Vertrauenswürdigkeit besitzen und Vertrauen gewinnen.

Sowohl die ***eSociety*** (i.e. die breite soziale Nutzung des Internets) als auch die ***eEconomy*** (i.e. die breite wirtschaftliche Nutzung des Internets) hängen ganz wesentlich von objektiver Vertrauenswürdigkeit und subjektivem Vertrauen in die internetbasierten Kommunikation und Interaktion und in die die Abwicklung von Transaktionen über das Internet ab.

Positive Kontextfaktoren (Stärken)

Das Window of Opportunity existiert aus drei Gründen: Erstens sind sehr viele Kontextfaktoren günstig. Die Technologie existiert und erhöht grundsätzlich den Komfort, weshalb ihre Nutzung attraktiv ist. Ein grosses generelles Grundvertrauen in Wirtschaft, Gesellschaft und staatliche Institutionen ist vorhanden. Es wird durch die Schweizer Tradition der Handschlagqualität, durch den in der Schweiz kulturell etablierten Willen zur Compliance und durch die hohe Qualität – i.e. Korrektheit, Fairness, Zuverlässigkeit, Effektivität und Effizienz – der Leistungen staatlicher Institutionen in der Schweiz gerechtfertigt. Dass die institutionelle Sicherheit und die politische Stabilität generell sehr hoch sind garantiert, dass dies auch in Zukunft so bleiben wird – wobei der weit verbreitete Pragmatismus zu einer vergleichsweise hohen Flexibilität im Rahmen stabiler politischer Zustände sichert.

Weiters ist das Interesse in der Schweizer Bevölkerung an Sicherheit und damit an der Nutzung der entsprechenden Technologie grundsätzlich hoch. Eine entsprechend sichere Internetkommunikationsinfrastruktur ist in vielen Bereichen bereits vorhanden. Die staatlichen Institutionen verfügen überdies über qualitativ hochwertige Informationsbestände. Der Bildungsstand der Bevölkerung ist hoch und die Nutzung von Informations- und Kommunikationstechnologie ist sehr weit verbreitet – bei Jugendlich sogar annähernd zu 100%. Das alles schafft sehr günstige Kontextfaktoren.

Zweitens steht mit der SuisseID eine einfache Lösung mit praktisch unbeschränkter Skalierbarkeit zur Verfügung, die universell einsetzbar ist. Die Bescheidenheit des Konzepts ist seiner grossen Stärken.

Drittens wird die SuisseID nicht nur vom Bundesrat und von einigen Akteuren im öffentlichen Sektor gepuscht, sondern auch die Bereitschaft der Wirtschaft ist 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, denn trotz einiger exzellenter Lösungsansätze im Ausland für vertrauenswürdige Internetinteraktionen, konnten dort die implementierte Lösungen nie die Anwendungsfelder eSociety und eEconomy substanziell durchdringen. In den meisten Fällen sind sogar nach mehreren Jahren die Nutzerzahlen gering und die Nutzungen eher marginal. Zudem hat die Dynamik von Neuentwicklungen in den Ländern ohne funktionsfähige Lösungen stark nachgelassen.

Negative Kontextfaktoren (Schwächen)

Es gibt verschiedenste Gefahren, die dazu führen könnten, dass sich das Window of Opportunity schliesst, bevor es genutzt werden kann. In solch einem Fall könnte eine gescheiterte SuisseID eventuell sogar zu einer Blockade für die Entwicklung von eEconomy und eSociety in der Schweiz für die nächsten Jahre werden. Konkrete Gefahren sind unter anderem, dass

a. die ökonomische Grundlage unsicher ist, weil die Unternehmen der Wirtschaft für eine erhöhte Vertrauenswürdigkeit nicht zahlen wollen (bzw. KMUs gar nicht über die nötigen Ressourcen verfügen) und weil Geschäftsmodellen für den Verkauf von mehr Sicherheit und Vertrauenswürdigkeit fehlen
b. die föderale Zersplitterung die gemeinsame Nutzung von Standards, Konzepten und Werkzeugen erschwert, die politische Führung im föderalen Kontext fehlt und eine grosse Ohnmacht gegenüber den marktbeherrschenden Unternehmen von den politischen Akteuren empfunden wird, welche den Elan bremst
c. die Registerdatensituation noch nicht bereinigt wurde, es keine reifen und genügend reflektierten Governance-Mechanismen für den Umgang mit Identitätsinformation gibt und eine Tradition der Sanktionen gegen Missbrauch fehlt
d. die Technologie zwar vorhanden ist aber schwierig zu nutzen und dass Akzeptanz und Nutzung neuer Dienste für mehr Sicherheit und Vertrauenswürdigkeit gering sind
e. bei vielen entscheidenden Akteuren im öffentlichen Sektor grosse Zweifel bestehen an der Möglichkeit eines nachhaltigen Erfolgs der SuisseID.

Systeminterne Stärken und systemexterne Chancen

Aus all diesen Überlegungen leitet sich die Frage ab, was getan werden kann, damit das Window of Opportunity genutzt werden und in eine nachhaltige, sich selbst begründende Entwicklung transformiert werden kann. Wichtiger als Schwächen zu beheben, ist es sicher, die Stärken weiter auszubauen. Statt auf das Ungeheuer „fehlende Geschäftsmodelle“ zu starren, sollte z.B. die genuin Schweizerische Tradition des guten Willens zum Mitmachen bei Innovationen genutzt werden. Es gilt die vorhanden Chancen zu Nutzen und die Risiken zu vermeiden, dabei aber auch in die Kraft eines SuisseID-Grooves zu vertrauen.

Spezielle Chancen sind unter anderem, dass

a. die SuisseID offen ist für neue Anforderungen, weil sie auf einem minimalen, einfachen und offenen Konzept basiert, dass multiple Identitäten, revozierbare Anonymität und eigenschaftsbasierte Rollen unterstützt und für eBusiness wie für eGovernment gleichermassen geeignet ist
b. die SuisseID sich politischen und geschäftlichen Trends flexibel anpassen kann, weil ihr Einsatz einerseits realen ökonomischen Nutzen bringt und sich andererseits gegenüber dem Kantönligeist neutral verhält (er kann ihn überwinden wie auch unterstützen helfen) – und weil viele neue Dienste in der öffentlichen Verwaltung ermöglicht und neue Geschäftsfelder für Unternehmen in einem sehr weitgehend offenen Gestaltungsraum (einem sogenannten „blauen Ozean“) eröffnet werden
c. negative Vorfälle das Bewusstsein für die Problematik in der einen oder anderen Form sowohl bei Bürgern und KMUs als auch bei den Geschäftsleitungen der grossen Finanzdienstleister wesentlich verstärkt haben und potentiell in Zukunft weiter verstärken werden
d. es intensive Bemühungen auf internationaler Ebene gibt (z.B. im Pilot-A-Projekt STORK des CIP PSP der EU, aber auch im aktuellen CIP PSP Call), die Beschränkungen für organisations- und staatsübergreifende Zusammenarbeit durch Standards für sichere Interoperabilität zu überwinden – und die SuisseID an die in Entwicklung befindlichen Lösungen andocken und so ihren Wirkungsbereich beträchtlich vergrössern konnte

e. der Bedarf für vertrauenswürdiges Management von identitätsbezogenen Informationen steigen wird und angesichts der Konkurrenzsituation es realistische Chancen gibt, dass die Schweiz hier in näherer Zukunft eine weltweite Spitzenposition einnehmen kann
f. das Vertrauen in die Schweiz als sicherer Hafen angesichts der europäischen Finanzturbulenzen wieder am Wachsen ist

Reale und imaginäre interne Gefahren und externe Risiken

Den Chancen stehen leider unterschiedlichste Gefahren gegenüber. Der private Bereich und der Geschäftsbereich sind sehr unterschiedlich und Fun-Probleme in ersterem könnten sinnvolle Entwicklungen in letzterem blockieren. Es liegt weiters in der Natur einer intensiveren IKT-Nutzung, dass sie das Missbrauchspotential vergrössert und dabei gleichzeitig das Bewusstsein um die Gefahren schwindet, beziehungsweise bei jungen Digital Natives gar nicht entsteht, und es liegt in der Natur der Weiterentwicklung von Vertrauenswürdigkeitstechnologie, dass sie auch ganz neue Möglichkeiten des Missbrauchs eröffnet – nämlich überall dort, wo sie nur scheinbar funktioniert, beziehungsweise die Einbettung in den Nutzungskontext nicht mit der nötigen Vorsicht erfolgt.

Die Erfahrung zeigt, dass ein Teil dieser Gefahren vorausgesehen werden, ein Teil aber immer erst durch Beobachtung der tatsächlichen Nutzung identifiziert werden kann. Mögliche schwerwiegende Missbrauchsfälle stiften zudem nicht nur Schaden an sich, sondern sie können auch dazu führen, dass das Misstrauen in den sinnvollen Gebrauch der Technologie wächst.

Die Komplexität der Thematik ist hoch und ihre anschaulichen Beschreibung schwierig. Das kann zu Verwirrung führen. Überdies ist das Gefahrenwissen bei Digital Natives gering und die Bequemlichkeit der unsicheren Internetnutzung untergräbt ganz generell die Bereitschaft zu einer vernünftigen Nutzung von Sicherheitstechnologie.

Dass die SuisseId wirklich für Benutzer attraktiv wird, breite Akzeptanz bei Unternehmen, Behörden und Bürgern findet und zum Selbstläufer wird, solange die wichtigsten Akteure in Politik und Wirtschaft noch dahinter stehen, setzt voraus, dass die vorhandenen Nutzungsmöglichkeiten schnell genug wachsen werden. Dies ist zurzeit mehr als fraglich. Schon jetzt ist absehbar, dass manch Übereifer zur Implementierung von technisch-organisatorisch mangelhaften Lösungen führen wird. Verzettelung und das Aufkommen verschiedenster Ängste – z.B. vor einem Kontrollverlust des Staates oder umgekehrt vor der Kontrollwut des Staates – sind wesentliche Risiken. Ebenso stellt die eingeschränkte Prognostizierbarkeit der Marktentwicklung ein Risiko dar.

Last but not least ist unklar, ob der Bundesrat den nötigen langen(sic!) Rückhalt bieten wird, bis das Window of Opportunity sich in eine nachhaltige Verbesserung der Voraussetzungen für eine blühende eSociety und eEconomy transformiert hat.

Liste der Empfehlungen

1. Governance durch partizipativ entwickelte Standards
2. Internationale Interoperabilität
3. Nutzerfreundliches Recht schafft vertrauen
4. Die öffentliche Debatte starten – awareness und Wisdom of the Crowd
5. Wissen schafft Kompetenzen – Kompetenzen schaffen Sicherheit – Sicherheit schafft Vertrauen
6. Vom schnellen Erfolg zur Nachhaltigkeit
7. Kein Vertrauen ohne Usability
8. Versicherung schafft Vertrauen
9. Schweiz 3.0 als Zentrum für Veranstaltungen und Institutionen
10. Keine Nachhaltigkeit ohne Forschung und Entwicklung

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.

Eine breit abgestützte, partizipative Entwicklung von Standards (wie sie von eCH vorgelebt wird) ist in dreierlei Hinsicht von Nutzen: Sie ermöglicht eine sehr umfassende Nutzung des vorhandenen Wissens. Sie schafft eine geteilte Ownership, die eine Verbreitung auf unterschiedlichen Kanälen ermöglicht. Und einer Ablehnung eines Standards als fremder Fötzel, respektive als Bundesberner Vorgabe, 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 schaffen

Wir empfehlen eine Öffnung der Schweizer eEconomy und eSociety für den sicheren elektronischen Verkehr mit dem Ausland,, indem die sichere Anwendbarkeit der SuisseID im Ausland und die sichere Nutzung ausländischer elektronischer Identitäten in der Schweiz 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 zwischen sicheren Systemen im In- und Ausland und sicheren Systemen im Ausland im Missbrauchsfall eine bessere reaktive Identifikation von Tätern und Verantwortlichen ermöglicht.

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

Empfehlung 3 – Nutzerfreundliches Recht schafft Vertrauen

Wir empfehlen die Quellen von Misstrauen im Schweizer Rechtssystem systematisch trocken zu legen. Bürger und KMUs sollen Vertrauen fassen, dass der Staat Fairness garantiert 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 wir, die Einsetzbarkeit vertrauenswürdiger Instrumente wie der SuisseID im öffentlichen Recht abzustützen.

Aktion 3.1
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 3.2
Die im Gesetz festgelegten Risiken der Bürger bei der Nutzung von Instrumenten wie der SuisseID sollen eingeschränkt werden.

Aktion 3.3
Präzedenzfälle sollen durch den Datenschutzbeauftragten 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 Akteure mit Missbrauchsabsichten wird aber die Sicherheit erhöhen, also die objektiven Voraussetzungen für Vertrauen verbessern.

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 partizipativ zu Governance-Lösungen zu kommen, die auf dem Wissen und den Erfahrungen der vielen, das heisst der Masse der Internetnutzer, beruhen. Diese öffentliche Debatte, welche Risiken wir einzugehen bereit sind, sollte von Regierungen, Parteien und Interessensorganisationen durch Wahrnehmung und Feedback gefördert werden.

Darüber hinaus sollten verschiedenste mehr oder weniger leise geäusserte Proteste innerhalb der öffentlichen Verwaltung gegen das besondere, nicht sehr verwaltungskulturkonforme, Vorgehen bei der Entwicklung der SuisseID ernst und zum Anlass einer Debatte genommen 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.

Aktion 4.2
Massnahmen sollten im Parlament und in der breiten Öffentlichkeit diskutiert werden, um dem grundsätzliche Recht, zu wissen wer über einen Daten sammelt, nachhaltig praktische Geltung zu verschaffen.

Aktion 4.3
Im Rahmen einer behördenintern offenen Debatte sollte eine Fallstudie über die SuisseID in Form einer SWOT-Analyse durchgeführt werden, um auch bei zukünftigen Vorhaben flexibler als bisher und zugleich ohne grössere Risiken als bisher handeln zu können. Damit könnte man auch proaktiv mit verschiedensten Ressentiments gegen das Projekt SuisseId umgehen, die zukünftige Weiterentwicklungen zu behindern drohen.

Empfehlung 5: 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. Insbesondere ist auch das Wissen über die SuisseID selbst bei E-Government-Insidern 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 nicht nur 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 5.1
Eine 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 das Bewusstsein geschärft, sondern es sollen auch Kompetenzen vermittelt werden. Diese Aktion hat erste Priorität!

Aktion 5.2
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 5.3
Die Anstrengungen zur Vermittlung von Wissen über die SuiiseID sollten massiv verstärkt werden. Diese Aktion hat grosse Dringlichkeit!

Aktion 5.4
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 5.5
Die Nutzung der Hochschuldienste sollte für möglichst viele Studierende – insbesondere auch solche aus der Weiterbildung – geöffnet werden.

Empfehlung 6 – 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 Informationsintermediärs für Identitätsmanagement-Informationen zu etablieren. Dieser soll eine sicheres Upscaling des Systems entstehender Dienste ermöglichen. Wichtig wäre weiters, dass die Bundesregierung und die Kantonsregierungen ihr Commitment zum Thema SuisseID im Speziellen und zur Weiterentwicklung von eSociety und eEconomy geben.

Aktion 6.1
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 6.2
Ein Firmenmitarbeiter-Verzeichnisdienst sollte etabliert werden, abgestimmt auf die UID (welche hoffentlich im Parlament angenommen wird).

Aktion 6.3
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 6.4
Neue Anwendungen der SuisseID ausserhalb des E-Governments sollte zudem lanciert, bzw. deren Lancierung sollte weiter gefördert werden. Beispielsweise sollten Dienste mit Altersnachweis (z.B. soziale Medien für 10-14-Jährige) gefördert und zur Darstellung des Potentials der SuisseID genutzt werden.

Aktion 6.5
Es soll ein Informationsintermediär etabliert werden, der eine zur SIX-Telekurs im Bankensektor analoge Rolle im Bereich des Indentitätsmanagements hat.

Aktion 6.6
Der Datenschutz sollte als Enabler von vetrauenswürdigen Diensten statt als Verhinderer von theoretischen Risiken auftreten.

Aktion 6.7
Die Nachhaltigkeit der Investitionen sollte durch einen nationalen CIO gestärkt werden, der als Broker, Koordinator und Kommunikator auftritt.

Aktion 6.8
Der Bundesrat und die Kantonsregierungen sollten ein langfristiges Committment zum Ausbau der

IT-Infrastruktur für eSociety und eEconomy geben.

Empfehlung 7: 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. Schwierig zu benutzende Werkzeuge finden keine Akzeptanz und sind per se nicht vertrauenswerweckend.

Aktion 7.1
Informationen über Probleme der SuisseID-Nutzer sollten gesammelt und analysierte werden und die Probleme möglichst asap gelöst werden. Dies betrifft alle Probleme: mangelhafte respektive missverständliche Informationsbereitstellung, schwierige Entscheidungen (Stick oder Karte), „Papierkrieg“, fehlende One-Stop Service-Qualität für Privatkunden, Probleme beim Einsatz innerhalb von Organisationen und deren Firewalls, et cetera.
Diese Aktion hat grosse Dringlichkeit!

Aktion 7.2
Guidelines für Usability von Identitätsmanagement-Werkzeugen sollten gemeinsam von Behörden, Wirtschaft und Hochschulen entwickelt werden. Dies gilt insbesondere für die Benutzerschnittstelle zur Eigendefinition der Zugreifbarkeit von identitätsbezogenen Daten in sozialen Medien, aber auch für andere Werkzeuge zur Verwaltung digitaler Identitäten in unterschiedlichen Kontexten.

Aktion 7.3
Eine Usability-Zertifizierung sollte für Identitätsmanagement-Werkzeuge angeboten werden.

Aktion 7.4
Der Zugang zu den Bildungs- und Forschungsintranets sollte stark vereinfacht werden.

Empfehlung 8: Versicherung schaffen Vertrauen

Bisher gibt es kaum Möglichkeiten, sich gegen Schäden aus dem Missbrauch von Identitätsinformationen zu versichern. Das trägt wesentlich zu einer Fokussierung auf präventive proaktive Massnahmen unter Ausschluss der Planung möglicher reaktiver Massnahmen bei. Diese präventiven Massnahmen können aber nie hundertprozentige Sicherheit bieten und teils ist das Verhältnis von Sicherheit versus Kosten schlicht generalpräventiv – entweder für die Ausübung von Geschäftstätigkeit oder für die Schaffung persönlicher Sicherheit. Wir empfehlen deshalb, dass entsprechende Versicherungsprodukte angeboten werden, die Schäden finanziell abdecken, 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. Unter anderem Versicherungen gegen Datenlecks.

Empfehlung 9: Schweiz 3.0 als Zentrum für Veranstaltungen und Instititutionen

Orte, die als internationale Veranstaltungszentren fungieren, haben in der Vergangenheit von dieser Funktion stets sehr nachhaltig profitieren, beispielsweise Basel vom Konzil. Denn 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 9.1
Die Schweiz sollte gezielt zu einem Zentrum für Informationsaustauschevents zu virtueller Indentität und zu Vertrauensintermediären werden. Insbesondere sollten internationale Experten-Konferenzen zu diesen Themen mit Wissenschaftern und Praktikern abgehalten werden. Diese Konferenzen sollten von Bundesrat und KdK unterstützt werden.

Aktion 9.2
Die Ansiedlung von NGOs mit Themenezug sollte gefördert werden.

Aktion 9.3
Es sollten Bar-Camps zum Thema virtuelle Identität, soziale Medien und Internet-Governance durchgeführt werden.

Aktion 9.4
Alle Aktivitäten unter Empfehlung 7 sollten durch ein Programm koordiniert werden. Ein geeigneter Titel wäre *Konzil 21 – Basel, Genf, Zürich*

Empfehlung 10: Keine Nachhaltigkeit ohne Forschung und Entwicklung

Ohne Forschung und Entwicklung ist längerfristig keine Nachhaltigkeit garantierbar. Derzeit gibt es drei grundsätzliche Defizite: Es fehlt in der Praxis der Überblick über den weltweiten Entwicklungsstand. Es fehlt weitgehend das Wissen über die tatsächlichen Verhaltensweisen der Nutzer. Und es wird wenig in die Entwicklung von einfach nutzbaren, neuen Werkzeugen investiert.

Die meisten Praktiker und 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.

Das Wissen über das tatsächliche Vertrauen in Internetinteraktion und über den praktischen Umgang mit der eigenen digitalen Identität 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.

Die Entwicklung neuer Werkzeuge, die tauglich für den Alltag wie er heute ist, geht langsam voran. Forschungs- und entwicklungsprojekte konzentrieren sich meist auf anspruchsvolle technische Innovationen. Bei der Entwicklung simpler Praxiswerkeuge gibt es hingegen wenig Innovation. Dies sollte geändert werden, wobei das Vorgehen bei der SuisseID – bei aller Problematik, das es aus Sicht der traditionellen Behördenkultur hat – durchaus Vorbild sein kann.

Aktion 10.1
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 10.2
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 10.3
Das Verhalten in Bezug auf die eigene digitale Identität im privaten und Unternehmenskontext sollte ganz grundsätzlich erforscht werden.

Aktion 10.4
Werkzeuge sollten entwickelt werden, die es Nutzern ermöglichen, ihre digitale Identitäten kontrolliert und so weitgehend wie möglich zu löschen. (Damit ist nicht das Löschen von Accounts gemeint, das in der Regel einfach ist, sondern das Löschen von Daten.)

Aktion 10.5
Kein Wasser predigen ohne es selber zu trinken: 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.