SWITCH, Werdstrasse 2, P.O. Box, CH-8021 Zürich
www.switch.ch

Stellungnahme von SWITCH zu den Fragen gemäss «Fragen und Vorschläge zur Auslieferung von Personenidentifizierungsdaten an IdP» der FedPol vom 25.11.2018/V02

Autoren/Version: Christoph Graf & Rolf Brugger, SWITCH / 10.12.2018v1

Zur Verwendung im Rahmen der Arbeitsgruppe des Bundesamtes für Justiz zur Begleitung der technischen und organisatorischen Einführung der E-ID

1 Anforderungen aus der Zielsetzung

1.1 Uneingeschränkter Einsatz der E-ID

- Mit OIDC dynamic client registration wird grundsätzlich jegliches Endsystem erlaubt. Dieses Verfahren stellt die geringste Hürde für vertrauende Dienste dar, unterstützt somit die uneingeschränkte Nutzung der E-ID maximal, und könnte ohne vorgängige Registration bei einem IdP umgesetzt werden. Wir begrüssen dieses Vorgehen aus diesen Überlegungen. Anzumerken ist aber, dass es den Annahmen über ein Business Model gemäss Botschaft widerspricht.
- Statische Registrierung bei allen IdP ist mit guter Tool-Unterstützung realisierbar. SWITCH setzt hierfür eine selber entwickelte «Resource Registry» ein. Protokolle mit nativer Föderationsunterstützung (wie SAML) sind für solche Anwendungsfälle besser geeignet.
- Anpassungen auf Protokollebene sind nach Möglichkeit zu unterlassen. Deshalb empfehlen wir von der Dritten Variante abzusehen.
- Wir möchten ferner auf mehrere aktuell laufende Standardisierungsbestrebungen hinweisen, wie OIDC um (die bei SAML bereits vorhanden) Föderationsfunktionalität erweitert werden soll. Damit würden die angesprochenen Protokollerweiterungen hinfällig.

1.2 Einfachheit des Einsatzes

Stellungnahme zur Einheitlichkeit des «Buttons»:

- Die Bereitstellung eines staatlichen Logos für die E-ID ist grundsätzlich sinnvoll und soll durch vertrauende Dienste genutzt werden können. Damit kann zum Ausdruck gebracht werden, dass dieser Dienst die staatlich anerkannten E-IDs akzeptiert.
- Für die Weiterleitung zum «richtigen» IdP ist jedoch ein Verfahren vorzuziehen, das auf der Auswahl des eigenen Anbieters beruht. Dies kann durch einen separaten Discovery Service oder durch Embedding bei den Services realisiert werden. SWITCH setzt beide Methoden seit Jahren für die eigene Föderation mit über 1300 Services und 80 IdPs (international sogar bei mehr als 2000 IdPs) erfolgreich ein.

- Unterscheidung nach Sicherheitsstufe ist zu unterlassen. Dies ist dem IdP des Endkunden zu überlassen und kann sich je nach eingesetzter Technik stark unterscheiden.
- Unterscheidung nach staatlich anerkannt, resp. nicht anerkannt ist zu unterlassen. Für den Endkunden ist relevant möglichst einfach herauszufinden, was zu tun ist.
- Die GUI-Regeln sollen sich auf die Verwendung des E-ID-Logos sowie die Darstellung der anerkannten IdPs beschränken (sofern letzteres aufgrund der Technologiewahl überhaupt noch notwendig ist).

1.3 Einheitliche E-ID Identifikatoren

Auf einen solchen E-ID Identifikator ist nach Möglichkeit zu verzichten. Die Wahl des «richtigen» IdP kann auch ohne einen solchen Identifikator geschehen. SWITCH verwendet für die eigene Föderation keine solchen Identifikatoren. Je nach Anzahl Anbieter können Anbieter-Logos, Drop-Down-Listen oder andere Discovery-Mechanismen eingesetzt werden.

1.4 Einfache Integration E-ID nutzender Dienste

Bei vertrauenden Diensten bereits verwendbare Protokolle stellen eine grosse Investition dar. Bei SWITCH sind zum Beispiel mehr als 1300 Services für SAML gerüstet, jedoch nicht für OIDC. Es ist unrealistisch, dass eine grössere Anzahl dieser Dienste alleine für die E-ID Funktion ein weiteres Protokoll implementieren wird.

Es wäre hingegen gut vorstellbar, dass Anbieter, wie z.B. SWITCH, Gateways bereitstellen, um die Anbindung an ihre jeweiligen Dienste zu ermöglichen. Der IDV könnte ähnlich vorgehen wollen. Möglicherweise müssen diese Gateways in einem Vertrauensverhältnis zu den angeschlossenen vertrauenden Diensten stehen und würden alle anerkannten E-IDs akzeptieren.

Die staatliche E-ID hat ein vorgegebenes Set an zwingend vorzuhaltenden Attributen. Es ist wichtig, dass dieses klar umrissen und stabil ist. Eine Anreicherung mit zusätzlichen optionalen Attributen aus anderen Anwendungsbereichen betrachten wir auf Ebene der E-ID als nicht realistisch umsetzbar. Geeigneter erscheint uns hier ein bilateral vereinbartes Vorgehen zwischen einzelnen IdPs.

Ein Beispiel: Verschiedene IdP könnten verschiedene Attribute liefern – ein Health-Professional-Status wäre dann halt nur mit einer HIN-ID zu haben, oder der Studierendenstatus nur über die SWITCH edu-ID. Werden in Anwendungsfällen beide Attribute gleichzeitig benötigt, können sich die IdPs bilateral absprechen.

Zu berücksichtigen ist ferner, dass die Anmeldung eines vertrauenden Dienstes bei einem IdP in der Regel nicht alleine in der Absicht erfolgt die E-ID zu akzeptieren. Dies erfolgt in aller Regel im Kontext der Nutzung weiterer Dienstleistungen.

Die Plastik-IDK kann von jedem vertrauenden Dienst ohne vorgängige Registration einsetzt werden und basiert auf den gleichen Registerdaten. In Anlehnung daran könnten auch Methoden vorgesehen werden, die gar keinen Vertrag bei einem IdP voraussetzen (siehe auch Kapitel 1.1).

1.5 Einheitliches Format und Semantik für Identitätsattribute

Absolut zentral ist die vereinheitlichte Semantik der zwingend vorzuhaltenden Attribute.

In vielen Fällen des E-Commerce wird der IdP nebst staatlich geprüften Attributen weitere zusätzlichen Attribute aus anderen Quellen an vertrauende Dienste liefern. Dabei ist es für den vertrauenden Dienst oft unerheblich, ob die Qualität einzelner Attribute staatlich beglaubigt ist oder nicht, solange die mit dem jeweiligen IdP vereinbarte Qualität über die Gesamtheit der Attribute erreicht wird.

1.6 Sicherheitsmechanismen

Wir sehen keine zwingenden Gründe für den Einsatz einer neuen PKI.

Ohne zwingende Gründe sollen keine über die standardmässigen Sicherheitsmechanismen hinausgehenden Methoden eingesetzt werden.

1.7 Datenschutz und Privatheit

Wir betrachten den E-ID-RN als technischen Identifikator, der nicht an Services weitergegeben werden soll. Dieser soll lediglich im Verkehr mit dem SID, sowie zur Verknüpfung mit der E-ID verwendet werden. Allfällige andere bei IdPs bereits bestehenden oder neue Identifikatoren der E-ID sollen durch die staatliche Anerkennung nicht zu sektoriellen EPID aufgewertet werden, auch wenn sie möglicherweise eineindeutig mit einer E-ID-RN verknüpft sein könnten. Im Streitfall sind sie nicht über den SID auflösbar, jedoch stehen hier andere Prozesse bereits zur Verfügung.

1.8 Initiale Identifizierung, Übermittlung der PID

Eine Testumgebung ist für potenzielle IdP ein wichtiges Instrument. Sei es für Tests im Rahmen der Bereitstellung der eigenen Lösung, aber auch als Testumgebung bei neuen Releases oder Verfahren, sowohl seitens des SID als auch der IdP.

2 Weitere Fragen seitens SWITCH

2.1 Annahmen betreffend des Business Models

In der Botschaft geht man davon aus, dass die vertrauenden Dienste als Hauptnutzniesser die Kosten der E-ID tragen sollen. In der Folge davon werden bei der Überwälzung der Kosten des SID Überlegungen angestellt, die möglicherweise nicht kostenorientiert sind. Wir gehen davon aus, dass die initiale Registration ein wesentlich aufwändigerer Prozess ist, als der periodische Abgleich der Attribute. Dennoch wird erwogen den Initialprozess, im Gegensatz zu den periodischen Abgleichen, unter gewissen Bedingungen gratis anzubieten.

Wir möchten einen potenziellen Anwendungsfall skizzieren: Für neue Identitäten (z.B. im Rahmen einer Immatrikulation) könnten wir staatlich geprüfte Identitäten ausstellen. Wir belasten die Individuen nicht und könnten auf Kostenfreiheit gegenüber dem SID zählen. Da nach einem Jahr die Immatrikulation wohl abgeschlossen ist und die Kundenbindung tragfähig geworden ist, kann die E-ID-Funktion an Bedeutung verlieren. Somit verzichten wir auf den Abgleich nach einem Jahr, lassen die E-ID erlöschen und bezahlen weiterhin nichts. Wie beurteilen sie diesen Anwendungsfall im Lichte des in der Botschaft skizzierten Business Models?

2.2 Monopolbildung

Wie würde sich das BJ bei der Situation verhalten, wenn sich nur ein einzelner Anbieter zur Herausgabe einer staatlich anerkannten E-ID entschliessen sollte. Würde das BJ dies als Versagen des Marktkonzeptes interpretieren?

Jedenfalls würde dies die Komplexität stark reduzieren, indem die Anforderungen an die Interoperabilität hinfällig werden. Jedoch würde dies dem ordnungspolitischen Ruf nach einer direkten Vergabe Vorschub leisten.

2.3 Bewertung von Umsetzungszielen

Soll folgendes Szenario unterstützt werden?

Hauptsächlich e-Gov-Angebote verwenden die E-ID als vertrauender Dienst für Logins ihrer Kunden. Andere vertrauende Dienste verwenden die E-ID in vielen Fällen lediglich als Hilfestellung bei der Erstellung eines Kundenkontos.