Besprechungsergebnis

Sektorkomitee ITS - Gruppe ZertES/PKI

Datum	20.10.2022	Anwesend	Thomas Hilger (SAS) Susan Omondi (SAS) Reto Grubenmann (KPMG) Reto Scagnetti (Digicert) Philipp Wirth (KPMG) Christian Jenny (BAKOM) Michael Guenther (Swisssign) Michael Widmer (Swisssign) Tobias Bertschi (Swisssign) Sandra Wuilloud (BAKOM) Paul Andermatt (BAKOM) Lucas Prêtre (BAKOM) Mario Lovisi (BIT) Stephanie Schäfer (BIT) Peter Stadlin (SAS) Rafael Knecht (Swisscom) Ingolf Rauh (Swisscom) Urs Würgler (Swisscom) Enke Cornelia (Digicert)
Ort	SECO/SAS HO36-2.U06 3003 Bern	Entschuldigt	von Niederhäusern Michael (BIT) Peter von Dach (BK-DTI) Frutiger Bruno (BK) Torsten Kahlstadt (Swisssign) Jos Doekbrijder (SWIS)
Zeit	13:00 – 16:30h	Protokoll	S. Omondi / Th. Hilger
Vorsitz	Thomas Hilger	z.K. an	gsn

Traktandum	Ergebnis, Entscheid
Protokoll	Das Protokoll vom 18.01.2022 wurde ohne Änderungen genehmigt und kann auf den Webpages der SAS publiziert werden.

Fragen und Erfahrungen neue TAV

1. **Begrüssung**

   Die unten aufgeführten und besprochenen Themen wurden von den TSP gewünscht und vorab ausformuliert – siehe auch die Agenda für das Meeting vom 20.10.2022

Traktandum	Ergebnis, Entscheid
2. Thematik rund um Given Name und Surname (insbesondere Folgen bei ausländischen Ausweisen, diakritische Zeichen etc. auch auf die Gültigkeit einer QES und Haftung)	**Ziel**: Verständnis und klare Auslegeordnung der TAV, Kap. 2.3.2 e und f). **(Hintergrundinformationen von Swisscom)**: Die neue TAV beschreibt abweichend von der Praxis und Regularien von ETSI und EU in Kapitel 2.3.2. e & f) die Notwendigkeit der Wiedergabe des „vollständigen Namens“ bzw. „sämtlicher Vornamen“ in den Attributen „surname“ bzw. „givenname“. Die Definition „vollständiger Name“ oder „sämtliche Vornamen“ greift tief in das national geprägte Namensrecht ein, da die Signatur in der Schweiz von zahlreichen Personen mit ausländischen Pässen genutzt wird. Alleine 25% der Wohnbevölkerung der Schweiz sind Ausländer, darüber hinaus werden Unterschriften stark im internationalen Austausch genutzt. Moderne Identifikationsverfahren nach ETSI TS 119 461, die nun auch in der Schweiz halten, setzen auch auf neue Verfahren, wie z.B. Autoidentifikation mit Auslesen des NFC Chips im Ausweis oder einer Identifikation durch das Bankkonto, bei dem die Bank die Metadaten der überprüften Person mitteilt. BAKOM interpretiert derzeit die Aussage der TAV als Darstellung des Namens gemäss der „Visual Zone des Ausweises“, welche aber nur teilweise korreliert mit den Daten im NFC Chip. Gerade im Ausland werden über 400 diakritische Zeichen verwendet, deren Lesbarkeit aufgrund der drucktechnischen Echtheitsmerkmale im visual Bereich „falsch“ gelesen werden können. Auch ist gesetzlich der Begriff „Name“ nicht definiert. Wie sieht es haftungstechnisch aus, wenn gegen 2.3.2 e) fehlerhaft oder aus Unwissenheit einer nationalen Namensgebung verstossen wurde? Das BJ fordert, dass alle Vornamen im Ausweis erscheinen müssen. Es wäre wünschenswert eine Europa-kompatible Lösung zu finden. Gefahr für TSPs: Haftung für nicht korrekte Auswertung. Unklarheiten u.a. betreffend: welche Namen relevant sind, Vorgang beim Abschneiden von Namen oder bei der Transkodierung, gleiche Regeln für NFC und MRZ-Daten, Interpretation und ggf. darauffolgende (manuelle) Korrektur, Pseudonyme als Lösung nicht nachvollziehbar, möglichst automatisiert, Kosten der Identifikationsverfahren, Akzeptanz der elektronischen Signatur in der Schweiz. Bezugnehmend auf: TAV 2.3.2 e & f) (Ausgabe 2, 17.02.2022) ETSI TS 119 461 (Ausgabe 2021-07) ETSI EN 319 412-2 (Ausgabe 2015-12) **Ergebnis**: keine Änderung in der TAV nötig. Die TSP und die Anerkennungsstelle könnten definieren, wie eine einheitliche Umsetzung erfolgen kann. Das BAKOM erinnert daran, dass die Erwähnung aller Vornamen im Zertifikat von zwei anerkannten TSPs sowie vom BJ insbesondere zur Gewährleistung der Rechtssicherheit gewünscht wurde. Das BAKOM

Traktandum	Ergebnis, Entscheid
	schlägt daher vor, das BJ zu konsultieren, um zu klären, ob auf die Erwähnung aller Vornamen im Zertifikat verzichtet werden kann und ob in diesem Fall eine Änderung der TAV erforderlich ist. Das BAKOM erinnert daran, dass nach dem ICAO 9303, Part 3-Standard Namen in der MRZ oder im Chip des Identitätsdokuments abgeschnitten werden können. Einige Zeichen wie das spanische «ñ» können kodiert werden (B.4.1 "*for example, the character "Ñ" can be transliterated into the MRZ as "NXX"»).* Das BAKOM ist der Ansicht, dass die anerkannte TSP in der Lage sein muss, diese Fälle während der Phase der Sammlung der für die Attribute *surname* und *given-name* zu übernehmenden Informationen zu identifizieren, damit die im Zertifikat erwähnten Namen mit den im VIZ-Bereich des Identitätsdokuments vorhandenen Namen übereinstimmen. Man könnte jedoch das Fehlen von Akzenten wie z.B. den im Französischen verwendeten «é», «è» tolerieren. **Nächste Schritte**: Das BAKOM wird das Bundesamt für Justiz (BJ) konsultieren. **Wer**: BAKOM **Bis wann**: vor der nächsten Besprechung, die ca. im April 2023 stattfindet.
<u>Nachtrag vom 13.01.2023:</u>	Das BAKOM hat am 24.11.2022 die oben erwähnte Besprechung mit den Verantwortlichen im BJ durchgeführt und es kann folgendes Ergebnis festgehalten werden: Aufgrund des hohen Sicherheitsanspruchs des Identifizierungsprozesses ist das BJ der Ansicht, dass die Identität der Zertifikatinhaberin oder des Zertifikatinhabers so präzise wie möglich formuliert werden soll. Daher sollten die Ziffern 2.3.2 e) und f) der TAV über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate unverändert beibehalten werden. Das BJ teilt die Einschätzung des BAKOM, dass die unter den erwähnten Ziffern verwendeten Begriffe «vollständiger Name» sowie «sämtliche Vornamen» gemäss deren Wortlaut auszulegen sind und keine extensivere Interpretation zulassen. Bestehen Unterschiede zwischen den Daten der VIZ, des Chips oder der MRZ, so sind die Daten der VIZ zu verwenden. Damit wird auch sichergestellt, dass die Datenerfassung weitestmöglich derjenigen entspricht, die für den elektronischen Identifikationsnachweis (E-ID) vorgesehen ist. Eine Änderung der TAV scheint dem BAKOM damit nicht angebracht, zumal der Inhalt des Textes von der Mehrheit der betroffenen Personen gleich interpretiert und verstanden wurde.
3. Thematik 119 461 – diese wird in der Schweiz (scheinbar) anders ausgelegt als in der EU (z.B. 100% Backgroundcheck bei KI gestützten Autoidentifikation)	**Ziel:** verstehen, warum die Auslegung in der CH anders ist als in der EU **Hintergrundinformationen von Swisscom**: Bei allen IDs, die kein NFC Auslesung ermöglichen, muss in der Schweiz ein 100% Background Check erfolgen. Internationale erprobte KI-Verfahren in der EU liefern aus Sicht TSPs Qualität und Schnelligkeit, aktuell aber nur mit Schweizerreisepass möglich, da Schweizer ID kein NFC erlaubt.

Traktandum	Ergebnis, Entscheid
	Bezugnehmend auf: ETSI TS 119 461 (Ausgabe 2021-07) REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 (EIDAS) **Ergebnis:** das BAKOM bestätigt, dass die Regeln der Spezifikation ETSI TS 119 461 für die Bewertung angewendet werden müssen. Der Fernidentifizierungsprozess ist konform, wenn sie die Anforderungen erfüllt. Bisher gibt es keine europäischen Regeln für die Fernidentifizierung. Es handelt sich um nationale Regeln (siehe Artikel 24, eIDAS), von denen einige auf der Spezifikation ETSI TS 119 461 basieren. Eine Europa-kompatible Lösung wird grundsätzlich angestrebt. **Nächste Schritte**: keine notwendig **Wer**: NA **Bis wann**: NA
4. SAM CC Evaluierung (gem. TAV 2.2.3 d)	**Ziel**: Wie ist die Vorgabe (TAV 2.2.3 d) zu interpretieren und auszulegen? **Hintergrund**: Unklar, wie ähnliche Sicherheitsziele wie jenen der Normen EN 419221-5 und EN 419241-2 interpretiert und geprüft werden sollen. Bedenken: Es kostet viel Zeit Prozess nach diesen Normen aufrechtzuerhalten: EN 419241-2 und EN 419221-5, Info BAKOM: Die neuen Normen ETSI TS 119 431-1, EN 419241-1, EN 419241-2 und EN 419221-5 wurden veröffentlicht und sind nun für die Prüfung von Signaturdiensten anerkannt. Daher wurden die TAV angepasst, um diesen Entwicklungen Rechnung zu tragen. Auf dem Markt gibt es Signaturdienste, die Systeme nutzen, deren Komponenten zuvor anhand anderer Kriterien in Bezug auf die Generierung von elektronischen Signaturen und Siegeln geprüft wurden. Diese Systeme werden als sichere Signatur- und Siegelerstellungseinheiten im Sinne von Artikel 6 Absatz 2 ZertES akzeptiert, sofern sie ähnliche Sicherheitsziele wie jenen der Normen EN 419241-2 und EN 419221-5 erfüllen. Wie in den europäischen Ländern, die Signaturdienste dulden, wird so ein Übergang gewährleistet, bis sich die Normen EN 419 241-2 und EN 419221-5 für die Evaluierung solcher Systeme durchgesetzt haben. Sobald dies der Fall ist, will die Europäische Kommission ihren Durchführungsbeschluss (EU) 2016/650 anpassen und diese neuen Normen darin aufnehmen. Letztere werden dann im Rahmen der Zertifizierung dieser Signaturerstellungseinheiten anwendbar sein. In der Folge werden die TAV ein weiteres Mal revidiert werden müssen, um die Anforderungen in der Schweiz an jene der europäischen Länder anzugleichen. Vorschlag Peter Stadlin (SAS): Die geforderten Protection Profiles als Basis nehmen und die Konformität sowie den Erfüllungsgrad der darin definierten «Security Functional Requirements» [SFR] mit ihren «Security Functional Components» bezüglich den spezifisch einge-

Traktandum	Ergebnis, Entscheid
	setzten Komponenten unter der Angabe des Evaluationsgrades (EAL) mit den dazugehörenden SARs dokumentieren **Entscheid**: Der Ausdruck «ähnliche Sicherheitsziele» bleibt. Die Evaluation soll gemäss oben stehendem Vorschlag als Prozess durchgeführt und dokumentiert werden. Die Dokumentation beinhaltet eine Liste mit den Security Functional Requiremts gemäss dem entsprechenden Protection-Profile und wird mittels Quervergleichen für die entsprechende Komponente (Target of Evaluation (TOE)) unter der Angabe des Evaluationsgrades (EAL) sowie mit dokumentierter Angabe des Erfüllungsgrads ausgefüllt. Bereits zertifizierte Komponenten (z.B. nach FIPS 140-2, FIPS 140-3) müssen selber nicht mehr evaluiert werden und sollen bezüglich ihren Security Functions in der Liste entsprechend den Security Function Requirements dokumentiert zugeordnet werden. Die Korrektheit und Anwendbarkeit einer solchen Dokumentation kann mittels einer Pre-Review und einer Erweiterungszertifizierung durch die Zertifizierungsstelle bestätigt werden. **Nächste Schritte**: N/A **Bis wann**: In der Verantwortung des TSPs
5. Validierung von signierten Dokumenten -- Validator.ch	**Ziel**: Das Bedürfnis nach einer automatisierten und diskreten Validierung (Dokumente verlassen das Unternehmensnetz nicht). **Hintergrund**: Kundenbedürfnis. Aktuell nur validator.ch, betrieben durch BIT. Stellungnahme der BK per E-Mail: Dieses Anliegen wurde seitens einer TSP in telefonischen Diskussionen mit dem Leiter Standarddienste verschiedentlich im zweiten Halbjahr 2021 platziert. Darauffolgend gab es etliche BV-interne Vorabklärungen in dieser Angelegenheit. Aktuell sind auf Seite BK diverse Abklärungen - auch mit dem BJ - gelaufen, um die Öffnung des Einsatzes des (Diskreten) Validators auch für Drittunternehmen und allenfalls Dritte (Privatpersonen) zu ermöglichen. Dazu müssten zuerst aber die dazu erforderlichen Voraussetzungen geschaffen werden. Das Ganze ist in diesen Tagen in eine Ämterkonsultation zu einem neuen Bundesgesetz über die Plattformen für die elektronischen Kommunikation in der Justiz (BEKJ) eingeflossen. **Ergebnisse**: Follow-up durch Bundeskanzlei (BK). **Nächste Schritte**: BK informiert ausserhalb dieser Sitzung **Wer:** BK/BJ **Bis wann**: in Verantwortung der BK
6. Umgang mit Minderjährigen: Wie soll mit der Ausstellung von Zertifikaten an Minderjährigen umgegangen werden? Ist eine Altersgrenze angedacht? Notwendigkeit des Beizugs von Erziehungsberechtigten?	**Ziel:** Umgang bei der Ausstellung von Zertifikaten an Minderjährige verstehen / definieren. **Hintergrund:** dieses Thema ist in der TAV/ im Gesetz nicht explizit abgedeckt **Entscheid:** Handhabung wie bei nicht digitalen Fällen. Geschäftsfähigkeit aus rechtlicher Sicht findet hier genauso Anwendung.

Traktandum	Ergebnis, Entscheid
(Swisscom)	**Nächste Schritte**: keine notwendig **Wer**: NA **Bis wann**: NA
7. Nutzung von Wettbewerbszertifikaten/QES zum Onboarding (analog EU-Gesetz) (Swisscom)	**Ziel:** Umgang mit Nutzung von Wettbewerbszertifikaten verstehen. Diese Regelung ist im Schweizer Gesetz nicht explizit erwähnt. Ist hier eine Änderung geplant? **Hintergrund:** In der EU werden auch Zertifikatsanträge zugelassen, die mit einer qualifizierten Signatur eines Wettbewerbers unterzeichnet wurden. Siehe Artikel 24, REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 (EIDAS) Art. 7 Abs. 3 Bst. b VZertES **Ergebnis:** Eine Änderung würde eine Anpassung der VZertES erfordern. **Nächste Schritte**: BAKOM wird beurteilen, ob eine Anpassung der Regel möglich ist. **Wer**: BAKOM **Bis wann**: April 2023
8. Diverses:	a. Meldung Peter Stadlin: Das SwissID-Zertifikat ist nicht RFC 5280 konform. Die Vorgaben der TAV 2.3.2 j bezüglich der Erweiterung des Attributs «admission» zur Angabe einer beruflichen Befähigung in der Standard-Zertifikatserweiterungsklasse {2 5 29} sind richtig. Das Attribut «admission» und seine Subattribute gehören unter die spezifische Standard-Zertifikatserweiterung «SubjectDirectoryAttributes» {2 5 29 9}. Gemäss Meldung Swisscom wurde dieses Attribut nicht verwendet. Der Hinweis wurde durch die Zertifizierungsdienstanbieter verdankt. b. Ist es möglich alle Anbieter von QES Dienstleistungen in der Liste der zertifizierten Unternehmen aufzunehmen? Wenn ja, wer übernimmt diese Aufgabe? Problematik: Diese Liste wäre sehr dynamisch und hätte eher einen Marketingcharakter. Die SAS kann eine solche Liste nicht unterhalten. Vorschlag: KPMG oder andere Möglichkeiten überprüfen oder TSP macht je eine Liste Das BAKOM stellt klar, dass die aktuelle Liste auf Art. 5 ZertES beruht. Es handelt sich um die Liste der anerkannten Anbieterinnen von Zertifizierungsdienste. Nach Art. 3 Abs. 1 Bst. b muss eine anerkannte Anbieterin von Zertifizierungsdienste in der Lage sein, qualifizierte Zertifikate gemäss ZertES auszustellen und zu verwalten. Man kann also nicht jeden beliebigen Anbieter in dieser Liste aufführen, auch wenn er zertifiziert ist. Eine weitere separate Liste wäre denkbar.

Traktandum	Ergebnis, Entscheid
	Nächste Schritte: N/A
9. Wunsch nach «Zulassung» eines weiteren Zertifizierers	**Ziel**: Zulassung weitere Zertifizierungsstellen für ZertES **Hintergrund**: Aus Sicht der TSPs würde mehr Wettbewerb sehr begrüsst. Begründung: Durch unterschiedliche KBS würde Qualitätsniveau gesteigert, mehr Flexibilität und schnellere Reaktionszeiten erwartet. (sowie die Tatsache, dass die Anzahl der Prüfkriterien durch den Einbezug der neuen ETSI erweitert hat) SAS erklärt die Grundlagen und den Prozess der Akkreditierung. Die Akkreditierung steht jedem Interessenten offen, der die Anforderungen erfüllt, z.B. - AkkBV - gesetzliche Anforderungen - int. Normen und Vorgaben - fachlich kompetent - unabhängig/unparteilich Hinweis: In der EU wurde der Wettbewerb unter Akkreditierungsstellen 2010 eingestellt, um eine einheitliche Qualität der Überprüfungen sicherzustellen. Man war der Ansicht, dass Wettbewerb sich über den Preis definiert und somit die Prüfqualität herabsetzt. Die SAS darf somit nicht einfach in anderen Ländern Akkreditierungsdienstleistungen anbieten. Aktivitäten mit akkreditierten ausländischen Stellen sind streng geregelt und erfolgen nicht ohne Zustimmung der verantwortlichen Akkreditierungsstelle je Land. **Ergebnis:** Der fehlende Wettbewerb liegt nicht an der SAS. Kriterien und Anforderungen müssen erfüllt werden. Unternehmen sind frei einen Antrag auf Akkreditierung zu stellen. **Nächste Schritte**: Keine notwendig Wer: NA **Bis wann**: NA
Nächste Sitzung und Themen	Nächster Termin: ca. April 2023. Doodle-Umfrage folgt Themenvorschlag: folgt rechtzeitig mit Hintergrund- und Ziel des Gesprächsthemas. Anregung BAKOM: je nach den zu besprechenden Themen andere Stakeholder wie z.B. Bereich «Digitale Transformation und Informations- und Kommunikationstechnologie (IKT)-Lenkung (DTI) und Bundesamt für Justiz einladen.

14.11.2022, S. Omondi SAS, Th. Hilger SAS