Protokoll zum Meeting vom 05.09.2024

Sektorkomitee ITS - Gruppe PKI

Datum Protokoll	21.10.2024	Anwesend	Thomas Hilger (SAS) Susan Omondi (SAS) Reto Scagnetti (Digicert) Philipp Wirth (KPMG) Christian Jenny (BAKOM) Sandra Wuilloud (BAKOM) Mario Lovisi (BIT) Ingolf Rauh (Swisscom) Oliver Zimmermann (Swisscom) Max Baumeister (Swisssign) Adrian Müller (Swisssign) Jos Doekbrijder (Swisgroup)
Ort	SECO/SAS HO36-2.U04 Holzikofenweg 36 3003 Bern	Entschuldigt	Lucas Prêtre (BAKOM) Peter Stadlin (SAS) Reto Grubenmann (KPMG) Stephanie Schäfer (BIT)
Zeit	14:00 – 17:00h	Protokoll	S. Omondi / Th. Hilger
Vorsitz	Thomas Hilger	z.K. an	Dr. Nicolas Guscioni

	Traktandum	Ergebnis / Entscheid
1.	Begrüssung und Traktanden Protokoll der letzten Sitzung	Das Protokoll vom 20.10.2022 wurde ohne Änderungen genehmigt und kann auf der Webseite der SAS publiziert werden. **Entscheid:** Neu wird das Protokoll zeitnah verschickt, Rückmeldung abgeholt und publiziert.
2.	Aufgaben des Sektorkomitees und Zusammensetzung	Die Aufgaben des Sektorkommittees besprochen und verstanden. Angehängt: File «Aufgaben Sektorkomitee ITS» **Entscheid:** Neu wird eine Ansprechperson pro Organisation eingeladen. Diese leitet die Infos weiter je nach Bedarf
3.	Entwicklungen in den Bereichen ZertES, VZertES, Trusted List und TAV-Revisionen, gegenseitige Anerkennung mit der EU.	Präsentiert von Christian Jenny. **ZertES:** Für das ZertES ist das Bundesamt für Justiz zuständig. Das eID-Gesetz wird eine Änderung des ZertES in Bezug auf die Identifizierung der Person, die ein Zertifikat beantragt, einführen. Künftig wird es möglich

	Traktandum	Ergebnis / Entscheid
		sein, sich mit einer gesetzeskonformen eID aus der Ferne identifizieren zu lassen. Das Inkrafttreten dieser Anpassung ist noch nicht bekannt. **VZertES und TAV**: Die Revisionen der VZertES und der TAV wurden gestoppt, da wichtige Revisionen von ETSI-Normen im Gange sind (TS 119 461, EN 319 411-x, EN 319 412-x) und es sinnvoll wäre, diese zu berücksichtigen. Es ist geplant, das Projekt im Herbst fortzusetzen. **Trusted List ist veröffentlicht.** Es ist wichtig das offizielle Formular des BAKOM zu nutzen, um Änderungen in der Liste zu beantragen. **Gegenseitige Anerkennung mit der EU:** Aktuell sind die Schweizer ZertES-Regeln mit den Europäischen eIDAS-Regeln nicht 1:1 vergleichbar. Das BAKOM hat einen Antrag an den Bundesrat vorbereitet. Eine Konsultation der Bundesämter ist noch erforderlich. Auf der Grundlage des Antrags sollte der Bundesrat das Mandat erteilen, Verhandlungen mit der Europäischen Kommission aufzunehmen. In der Zwischenzeit bereitet sich das BAKOM auf die Verhandlungen vor. Die umfangreiche Dokumentation, die der EU-Kommission vorgelegt werden soll, ist in Vorbereitung.
4.	Einhaltung vom MRA Cookbook der Europäisches Kommission (EC)	Präsentiert von Christian Jenny. Die Europäische Kommission (EC) hat das MRA Cookbook (https://eidas.ec.europa.eu/efda/international/trust-service?section=download_center) veröffentlicht. Dieses Dokument legt die Anforderungen für die gegenseitige Anerkennung von Trust Services zwischen der Europäischen Union und einem Drittland fest. Die Analyse dieser Dokumentation hat zwei Lücken aufgedeckt: a) Hinweis, dass der private kryptographische Schlüssel durch eine sichere Signatur- und Siegelerstellungseinheit (SSCD) geschützt ist (Kap. 3.1.1.3 MRA Cook Book; Kap. 2.3.2, g TAV). Gemäss TAV 2.3.2, g): Dieser Hinweis muss in Form eines Objektbezeichners (OID) gemäss ETSI EN 319 412-5, 4.2.2, angegeben sein (id-etsi-qcs 4). Die ETSI-Experten planen eine Änderung der ETSI-Norm EN 319 412-5. In Zukunft sollte entweder der vorhandene Hinweis auf eine nach eIDAS zertifizierte SSCD oder der neue Hinweis auf eine nach anderen Regeln zertifizierte SSCD verwendet werden. b) Übereinstimmung des Namens des CSP in der Trusted List (TL) mit dem Namen des CSP im issuer-Feld des Zertifikats (Kap. 3.1.1.2 MRA

	Traktandum	Ergebnis / Entscheid
		Cookbook, ETSI TS 119 612, 5.5.3, NOTE 4). Bei der Erstellung der ersten Version der TL wurden Inkonsistenzen zwischen den Namen festgestellt. **Ergebnis / Massnahmen durch BAKOM** Für a) Falls erforderlich, wird das BAKOM TAV 2.3.2, i) ändern, um die Anforderung zu präzisieren. Für b): Das BAKOM wird die TL gemäss ETSI TS 119 612, 5.5.3, NOTE 4 anpassen. Das BAKOM bittet die CSPs, dafür zu sorgen, dass die Namen in Zukunft (bei der Erneuerung von Zertifikaten oder bei der Einführung neuer Dienste) übereinstimmen.
5.	Themenliste Swisscom a) Ersatz der Namen in der Liste der PKI Dienste der Schweiz	Präsentiert von Ingolf Rauh a) Braucht es diese Liste noch? Gemäss BAKOM: Ja. Diese Liste ist nützlich, da sie von Menschen leicht interpretiert werden kann, während die Trusted List im XML-Format für Software gedacht ist. Aktuell wird die Liste durch die SAS gepflegt. Ansprechpersonen sind jedoch nicht aktuell. **Kurzfristig:** Thomas Hilger (SAS) macht einen neuen Vorschlag an KPMG. Es wird in Zukunft nur die Rollen der Verantwortlichkeiten und keine Namen eingetragen.
	b) Status Inkraftsetzung VZertES – falls noch nicht unter 3 beantwortet	b) Die aktuelle Version von 2.3.4 TAV weicht von der neuen Version des Konzeptes geregeltes Behördenzertifikat ab, welche auf der Website https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/digitale-kommunikation/elektronische-signatur.html publiziert ist. In der nächsten Version der TAV werden die im Konzept vorgenommenen Änderungen berücksichtigt. **Lösung:** das BAKOM wird auf ihre Webseite darauf hinweisen, dass die CSP die im Konzept vorgenommenen Änderungen bezüglich des Feldes „Organisational-Unit“ bereits anwenden können.
	c) Standard ETSI 319 401: Welche Version wird künftig massgeblich sein im Rahmen der TAV?	c) In den TAV wird nicht direkt auf die ETSI-Norm EN 319 401 verwiesen, sondern in der von ETSI implementierten Normenhierarchie kaskadiert. Die TAV enthalten einen spezifischen Verweis auf die ETSI-Norm EN 319 411-2, d. h. mit Angabe der zu berücksichtigenden Fassung dieser Norm. Diese Norm verweist auf EN 319 411-1, die wiederum auf EN 319 401 verweist. Die Angabe der Versionen der referenzierten Normen in den TAV ist ein Grundsatz, der vom Bundesamt für Justiz vorgegeben wurde. Um diesem Grundsatz gerecht zu werden, muss die zum Zeitpunkt des Inkrafttretens der TAV veröffentlichte Version der ETSI-Norm EN 319 401 berücksichtigt werden. **Ergebnis:** Keine Aktion notwendig.

	Traktandum	Ergebnis / Entscheid
	d) Standard ETSI 319 461: Welche Version wird künftig massgeblich sein im Rahmen der TAV?	d) In den TAVs findet man einen spezifischen Verweis auf die ETSI-Spezifikation TS 119 461, d. h. mit Angabe der zu berücksichtigenden Fassung. Das BAKOM möchte die neue Fassung der Spezifikation im Rahmen der Revision der TAV berücksichtigen. Die neue Fassung wird wichtige Anpassungen im Hinblick auf die Sicherheit des Identifizierungsprozesses enthalten. Eine Umsetzungsfrist ist vorgesehen. **Next step**: Das BAKOM fordert die CSP aber erneut dazu auf, diese Entwicklungen zu verfolgen und sich in geeigneter Weise darauf vorzubereiten.
	e) eIDASv2 Angleichung: Welche weiteren Anpassungen sind im Hinblick auf eIDASv2 im Rahmen ZertES/VZertES geplant?	e) **eIDASv2:** Aktuell noch beschränkte Angleichung an der EU-Änderung VZertES wäre notwendig. **Next step**: BAKOM nimmt dies auf
	f) Behördensiegel – Konzept	f) Für das Konzept des Behördensiegels ist die Bundeskanzlei zuständig. Die neueste Version des Konzepts ist auf der Website https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/digitale-kommunikation/elektronische-signatur.html veröffentlicht. Das BAKOM und die CSPs sind nicht mehr davon überzeugt, dass es notwendig ist, die Anforderung für das Feld „businessCategory“ beizubehalten, da diese Information redundant zum Feld OrganisationalUnit ist. Die Bundeskanzlei wurde um Erläuterungen und Argumente gebeten.
	g) GLEIF/vLEI: Wäre eine Zulassung des vLEI Vergabe- und Qualifizierungsprozesses im Rahmen VZertES möglich für die Vergabe geregelter Siegel an UID Einheiten, die eine vLEI aufweisen?	g) Die Verwendung eines offiziellen LEI-Registers zur Überprüfung der Daten der UID-Einheiten sollte möglich sein. Dazu müsste noch die Stellungnahme des BJ eingeholt und Artikel 6 Abs. 2 VZertES geändert werden. Um eine LEI in das Zertifikat aufzunehmen, müsste jedoch Art. 7 ZertES angepasst werden (Angaben im Zertifikat). Abs. 2 Bst e verlangt die UID-Nummer nach dem UIDG.
	h) Anerkennung von Identifikationsmethoden der EU, die von akkreditieren Konformitätsbewertungsstellen gemäss Verordnung 768/2005 und ETSI 319 403 der EU auditiert wurden und bereits zugelassen wurden im Rahmen von eIDAS	h) Erkenntnis: Anerkennung ist aktuell nicht gegeben. Stichprobe weiterhin sinnvoll, Evidenzprüfung durch eine akkreditierte Stelle notwendig.
6.	Spontane weitere Themen (jede/jeder mit Input/Frage)	Qualifizierter / geprüfter Validator wird durch die Bundeskanzlei betrieben.

	Traktandum	Ergebnis / Entscheid
		Next step: Mario Lovisi berichtet über Open Source Möglichkeiten beim BIT
7.	Nächste Sitzung und Themen	**Nächster Termin**: 11.09.2025 Themenvorschläge: bitte rechtzeitig mit Hintergrund- und Ziel des Gesprächsthemas einreichen. Anregung BAKOM: andere Stakeholder wie z.B. Bereich «Digitale Transformation und Informations- und Kommunikationstechnologie (IKT)-Lenkung (DTI) und Bundesamt für Justiz einladen. **Entscheid SAS**: Je nach Thema werden weitere TN ein Monat vorher geladen

21.10.2024, S. Omondi SAS, Th. Hilger SAS