A 4/2015-68

Bescheid

Die Telekom-Control-Kommission hat durch Dr. Elfriede Solé als Vorsitzende sowie durch Dr. Erhard Fürst und Univ.-Prof. DI Dr. Günter Haring als weitere Mitglieder aufgrund der Anzeige der A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH, Landstraßer Hauptstraße 5, 1030 Wien, vom 14.08.2015 in ihrer Sitzung vom 21.03.2016 einstimmig beschlossen:

I. Spruch

1. Die Tätigkeit der A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH als ZDA wird bei Einhaltung der nachstehenden Auflagen nicht untersagt:
   1.1. A-Trust hat bis zum 30.04.2016 eine finale, in sich konsistente und dem aktuellen Stand der Entwicklung entsprechende Systembeschreibung für das System der Handy-Signatur und seiner Schnittstellen zu erstellen und diese Systembeschreibung der Aufsichtsstelle zu übermitteln; überdies hat A-Trust bis zum 30.06.2016 das Sicherheitskonzept entsprechend zu adaptieren und der Aufsichtsstelle zu übermitteln.
   1.2. Auf Verbindungen zwischen Endgeräten des Signators und Rechenzentrum der A-Trust außerhalb des geschützten Bereichs des Rechenzentrums ist TLS 1.0 bis spätestens 30.06.2017 zu deaktivieren und stattdessen TLS 1.1 oder eine neuere Protokollversion einzusetzen. Die Aufsichtsstelle ist von der Durchführung in Kenntnis zu setzen.

TELEKOM-CONTROL-KOMMISSION
BEI DER RUNDFUNK UND TELEKOM
REGULIERUNGS-GMBH

A-1060 Wien, Mariahilfer Straße 77-79
Tel: +43 (0) 1 58058 - 0
Fax: +43 (0) 1 58058 - 9191
http://www.rtr.at
e-mail: rtr@rtr.at
FN: 208312t HG Wien
DVR-Nr.: 0956732 Austria

1.3. Die Implementierung des Diffie-Hellman-Verfahrens gemäß dem Dokument „A-Trust Handy-Signatur TAN-App Detailspezifikation“, Version 0.6 vom 14.03.2016, ist bis 30.04.2016 dahingehend anzupassen, dass [redacted]. Für eine rasche Verteilung der aktualisierten App ist Sorge zu tragen. Die Aufsichtsstelle ist unter Vorlage der aktualisierten Detailspezifikation von der Durchführung in Kenntnis zu setzen.

1.4. A-Trust hat eine externe Überprüfung der Sicherheit der gemäß Spruchpunkt 1.3 aktualisierten Handy-Signatur-App durchzuführen. Zu diesem Zweck sind der Aufsichtsstelle bis zum 30.04.2016 Vorschläge für derartige Tests und nach umgehender Freigabe durch die Aufsichtsstelle ehestmöglich, spätestens aber bis 30.09.2016 das Ergebnis zu übermitteln.

1.5. A-Trust hat auf ihrer Webseite Tipps und Empfehlungen zum Absichern mobiler Endgeräte durch Hinweise auf aktuelle Gefährdungen und Angabe von Virenscannern für jene Betriebssysteme, die dies unterstützen (Android, BlackBerry, Windows Phone) bekannt zu geben.

1.6. A-Trust hat bis zum 30.04.2016 für Registrierungsverfahren, bei denen eine Identifikation mittels [redacted] erfolgt, Prozesse zu implementieren,

1.6.1. die gewährleisten, dass die maschinenlesbare Prüfzeile des Lichtbildausweises des Signators systemgestützt ausgelesen und die Prüfziffer durch die [redacted]-Applikation nachgerechnet wird,

1.6.2. bei denen die Identitätsprüfung des Signators und die Sicherheitsmerkmale des von ihm verwendeten Ausweisdokuments photographisch dokumentiert werden und

1.6.3. bei denen der Einsatz von [redacted] oder anderen Services ungeprüfter Drittanbieter im Rahmen der Identifikation mittels [redacted] ab 1.07.2016 unterbunden wird.

1.7. A-Trust hat zu veranlassen, dass die Vertrauenswürdigkeit von [redacted] im Rahmen der Konformitätsbewertung durch eine Konformitätsbewertungsstelle bis spätestens 01.07.2017 beurteilt und im Anschluss das Ergebnis der Aufsichtsstelle übermittelt wird, insbesondere hinsichtlich

1.7.1. der Sicherheit gegen spezifische Angriffe mittels bild-/video-technischer Bearbeitungsmaßnahmen (insbesondere auch Sicherheit gegen Video-Echtzeitsimulationen),

1.7.2. der Anforderungen an Kameraqualität und Lichtverhältnisse für eine zuverlässige Prüfung der frei sichtbaren Sicherheitsmerkmale,

1.7.3. zusätzlicher Angriffsvektoren aufgrund der Verwendung video-basierter Komponenten und

1.7.4. etwaiger Mängel, die sich im Zuge der Zertifizierung oder Rezertifizierung der [redacted] nach ISAE 3402 ergeben haben. Zu diesem Zweck hat A-Trust durch eine entsprechende Vereinbarung mit [redacted] zu gewährleisten, dass Informationen über den im Zuge der Zertifizierung oder Rezertifizierung von [redacted] festgestellten Sachverhalt für A-Trust zugänglich sind.

2. Die Gebühr für die Prüfung der Änderung des Sicherheits- und Zertifizierungskonzepts wird gemäß § 1 Abs 1 Z 3 lit b SigV 2008 mit 3.000 Euro bestimmt. Die Gebühr enthält keine Umsatzsteuer. Die Gebühr ist von der A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH binnen zwei Wochen ab Zustellung dieses Bescheides an die Rundfunk und Telekom Regulierungs-GmbH, UniCredit Bank Austria AG, BLZ 12000, BIC BKAUATWW, Konto-Nr. 00696170109, IBAN AT451200000696170109, zu überweisen.

II. Begründung

1. Gang des Verfahrens

A-Trust zeigte mit Schreiben vom 14.08.2015 (ON 1) die Aufnahme des Zertifizierungsdienstes „EU-Identity Mobile“, Änderungen der Zertifizierungsdienste „a-sign premium“ und „a-sign premium mobile“ sowie Änderungen des Signaturdienstes „Handy-Signatur“ an. Mit Bescheid der Telekom-Control-Kommission vom 28.09.2015 wurde Frau Prof. Schaumüller-Bichl zur nichtamtlichen Sachverständigen bestellt (ON 17) und mit der Erstellung eines Gutachtens zur Sicherheit und zur Evaluierung der Sicherheit der von der A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH neu angezeigten bzw geänderten Signatur- und Zertifizierungsdienste bis zum 30.11.2015 beauftragt. Im Herbst 2015 wurden der Aufsichtsstelle vom deutschen Bundesamt für Sicherheit in der Informationstechnik („BSI“) und vom deutschen Bundeskriminalamt („BKA“) erhobene Bedenken im Hinblick auf die Verwendung des Video-Ident-Verfahrens zur Authentifizierung und Identifizierung von Personen bekannt, von denen A-Trust mit Schreiben vom 15.12.2015 (ON 43) informiert wurde. Diese Bedenken erforderten eine Beantwortung zusätzlicher, vom Umfang des bisherigen Gutachtensauftrags nicht abgedeckter Fragen und machten eine Erweiterung des bisherigen an Frau Prof. Schaumüller-Bichl erteilten Gutachtensauftrags, die mit Bescheid der Telekom-Control-Kommission vom 21.12.2015 (ON 46) erfolgte, sowie eine Erstreckung der Frist zur Gutachtenserstellung bis 18.01.2016 notwendig. Darüber hinaus übermittelte die Bestätigungsstelle A-SIT mit Schreiben vom 15.12.2016 eine bis auf Widerruf gültige Bescheinigung mit dazugehörigem Bericht zur Handy-Signatur sowie zur remote-signature Lösung OpenTrust Protect & Sign (ON 41). Frau Prof. Schaumüller-Bichl übermittelte ihr Gutachten samt Gebührennote (ON 50) am 18.01.2016. Nach Übermittlung von Gutachten und Gebührennote an A-Trust am 26.01.2016 (ON 53) nahm A-Trust mit Schreiben vom 12.02.2016 zum Gutachten Stellung (ON 54). Der dem Gutachten indirekt zugrundeliegende Artikel [redacted] wurde A-Trust am 16.02.2016 zur Stellungnahme übermittelt (ON 57a). Das Protokoll einer Telefonkonferenz zwischen Frau Prof. Schaumüller-Bichl und Prof. Haring am 26.02.2016 (ON 63) wurde A-Trust am 29.02.2016 zur Stellungnahme übermittelt (ON 64). Die Stellungnahme von A-Trust samt Beilagen (überarbeitete Belehrung der Signatoren, Screenshots zum Signiervorgang bei mehreren Dokumenten, überarbeitete Spezifikation der Handy-Signatur-TAN-App) langte am 14.03.2016 ein (ON 66).

2. Festgestellter Sachverhalt

Die Anzeige der A-Trust vom 14.08.2015 (ON 1) umfasst die Aufnahme des Zertifizierungsdienstes „EU-Identity Mobile“, Änderungen der Zertifizierungsdienste „a-sign premium“ und „a-sign premium mobile“ sowie Änderungen des Signaturdienstes „Handy-Signatur“. Der Zertifizierungsdienst „EU-Identity Mobile“ stimmt hinsichtlich der Angaben im Sicherheits- und Zertifizierungskonzept von A-Trust mit dem schon bisher angebotenen Zertifizierungsdienst „a.sign premium mobile“ weitestgehend überein. Das Konzept der Handy-Signatur wird insofern ausgeweitet, als die Übermittlung des Einmalpassworts für die Signaturerstellung nicht nur per SMS, sondern auch mit Hilfe einer Smartphone-App erfolgen kann. Überdies wird die Einführung eines weiteren Verfahrens zur Identitätsprüfung der Zertifikatswerber mit der Bezeichnung [redacted] angezeigt, bei dem die Identitätsprüfung eines Zertifikatswerbers von einem entfernten Standort aus mit Hilfe einer Webcam erfolgt.

Die angezeigten Dienste weisen in den nachstehend angeführten Punkten Mängel auf, aufgrund derer die Sicherheit der erbrachten Dienste nicht in ausreichendem Maße gewährleistet ist.

2.1 Systembeschreibung der Handy-Signatur

Das System der Handy-Signatur ist in einer Reihe von Einzeldokumenten (HLA, Detailspezifikation, Security Target, CP, CPS etc) beschrieben, die teilweise unterschiedliche Notationen verwenden und auch Inkonsistenzen aufweisen. Die Erstellung einer finalen, in sich konsistenten und dem aktuellen Stand der Entwicklung entsprechenden Systembeschreibung für das System der Handy-Signatur und seiner Schnittstellen zu den bestehenden Systemen erscheint daher geboten (ON 50, S 62).

2.2 Sicherheitsprotokolle

Das Sicherheitsprotokoll TLS 1.0 ist nach dem Stand der Technik nicht länger als ausreichend sicher anzusehen (ON 50, S 21). A-Trust hat mitgeteilt, die Unterstützung in TLS 1.0 für angreifbare kryptographische Algorithmen wie zB RC4 sei bereits deaktiviert worden, und angekündigt, es werde versucht, TLS 1.0 bis Jahresende gänzlich zu deaktivieren (ON 66).

2.3 Diffie-Hellman-Verfahren

A-Trust wendet für die Schlüsselvereinbarung zwischen HSM-Server und Handy-Signatur-App das Diffie-Hellman-Verfahren auf Basis sogenannter [redacted] an, die sich in der Form [redacted] darstellen lassen, wobei [redacted] (ON 66). Der Artikel [redacted] beschreibt in Abschnitt 3.3 einen Man-in-the-Middle-Angriff, bei dem [redacted] (ON 57a). Der beschriebene Angriff lässt sich im Fall der Verwendung von [redacted] nicht durchführen, wenn [redacted].

2.4 Externe Überprüfung der Handy-Signatur-App

Die Handy-Signatur-App wird von A-Trust entwickelt und getestet, eine externe Evaluierung der Software bzw eine Prüfung des Quellcodes fand bisher nicht statt. Wie bei allen Softwarekomponenten besteht auch hier die Möglichkeit, dass der Code fehlerhaft ist, aber auch, dass bewusst undokumentierte Funktionen (Backdoors) eingebaut wurden. Da das Restrisiko aufgrund der Vertrauenswürdigkeit und Qualifikation des Entwicklungspersonals als akzeptabel angesehen werden kann, reicht es aus, wenn eine externe Überprüfung der Handy-Signatur-App anstatt durch eine Quellcode-Überprüfung in Form von Black-Box-Tests erfolgt. A-Trust hält die Umsetzung von Black-Box-Tests innerhalb von drei Monaten für durchführbar (ON 66).

2.5 Belehrung der Signatoren

Nutzer der Handy-Signatur benötigen Sicherheitsempfehlungen für mobile Endgeräte, damit die Integrität der Handy-Signatur-App gewährleistet bleibt.

2.6 [redacted] – Prozesse bei der Identitätsprüfung

Durch visuelle Prüfung eines Ausweisdokumentes und Abfrage von benutzerbezogenen Informationen im Rahmen einer Videokonferenz wird von einem Mitarbeiter (Agenten) des

Call-Centers der [redacted] die Echtheit des Dokumentes, die Zugehörigkeit des Dokuments zur Person sowie die aktuelle Teilnahme an der Videokonferenz überprüft (ON 50, S 65).

2.6.1 Prüfzeile

Bei der Identitätsprüfung von Zertifikatswerbern durch die [redacted] müssen ausreichende Lichtverhältnisse und Übertragungsqualität nachweislich erfüllt sein, andernfalls darf das Verfahren nicht durchgeführt werden. Die Entscheidung darüber liegt beim [redacted]-Mitarbeiter (Agenten), der die Identifizierung durchführt. [redacted].

2.6.2 Photographische Dokumentation

Das im Rahmen der Identifikation des Zertifikatswerbers durch die [redacted] geführte Gespräch wird zur Gänze aufgezeichnet und ist damit auch zu einem späteren Zeitpunkt nachvollziehbar. Es werden Bilder vom Zertifikatswerber und vom Ausweisdokument angefertigt und gespeichert. Die Sicherheitsmerkmale [redacted] des Ausweisdokuments werden überprüft (ON 50, S 39).

2.6.3 Kommunikation mit dem Zertifikatswerber bei der Identitätsprüfung

Die Kommunikation zwischen dem Zertifikatswerber und [redacted] erfolgt auf zwei Kanälen, einerseits über eine Web-Applikation und parallel dazu über Verbindung über Videotelefonie ([redacted] oder WebRTC). Ein Vergleich der Sicherheit der Videoverbindung zwischen den beiden eingesetzten Systemen [redacted] und WebRTC zeigt, dass WebRTC aus sicherheitstechnischer Sicht aufgrund der Transparenz von WebRTC einerseits und möglicher Abhörschnittstellen bei [redacted] andererseits gegenüber [redacted] vorzuziehen ist (ON 50, S 45). Auch das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) fordert, dass keine unüberprüften Drittanbieter zum Einsatz kommen und benennt dabei als Beispiel [redacted] (ON 43). In Bezug auf die Video-Schnittstelle bestehen daher insgesamt starke Sicherheitsbedenken beim Einsatz von [redacted] (ON 50, S 67).

2.7 [redacted] – Beurteilung der Gleichwertigkeit von Videoident-Verfahren

Gegenüber einer Zustellung zu eigenen Handen bestehen bei Videoident-Verfahren grundsätzlich erhöhte Risiken (kein direkter Kontakt, keine Überprüfung der postalischen Adresse, uU niedrigere Hemmschwelle). Diesen stehen im [redacted]-Verfahren verstärkte Dokumentations- und Qualitätssicherungsmaßnahmen gegenüber, insbesondere Audioaufzeichnung des Identifizierungsvorganges, Bild der Person, die den Ausweis vorgelegt hat, Stichprobenprüfungen und Mystery-Calls (ON 50, S 65). Auch bei einer Zustellung zu eigenen Handen werden lediglich die mit freiem Auge sichtbaren Merkmale geprüft, sodass (mit Ausnahme der fehlenden haptischen Prüfmöglichkeit) die Echtheitsprüfung der Ausweisdokumente auf den gleichen Merkmalen beruht (ON 50, S 66).

Bei der Videoidentifikation können einige Umstände jedoch noch nicht abschließend beurteilt werden (ON 50, S 69). Dies sind insbesondere Sicherheit gegen spezifische Angriffe mittels bild-/videotechnischer Bearbeitungsmaßnahmen (insbesondere auch

Sicherheit gegen Video-Echtzeitsimulationen), Anforderungen an Kameraqualität und Lichtverhältnisse für eine zuverlässige Prüfung der freisichtbaren Sicherheitsmerkmale und zusätzliche Angriffsvektoren aufgrund der Verwendung video-basierter Komponenten.

Das BSI bereitet gegenwärtig ein Forschungsprojekt vor, in dem Voraussetzungen für eine Prüfung der optischen Merkmale mit hoher Qualität untersucht sowie verschiedene bild-/ videotechnische Manipulationsansätze analysiert und hinsichtlich ihres Aufwandes abgeschätzt werden. Ziele des Projektes sind die Feststellung der Manipulierbarkeit und die Analyse der Wirksamkeit möglicher Gegenmaßnahmen. Zusätzlich ist geplant, ein ausgewähltes Angriffsszenario im Rahmen dieses Projektes nachzustellen und zu dokumentieren (ON 50, S 57, 59).

Die [redacted] unterzieht sich Zertifizierungen nach ISAE 3402, wobei eine Zertifizierung vom „Typ 1“ (Eignung der eingerichteten Kontrollen zur Erreichung der Kontrollziele und Integration der Kontrollen in die Arbeitsprozesse) bis zum [redacted] und eine Zertifizierung vom „Typ 2“ (planmäßige Durchführung und nachvollziehbare Dokumentation der Kontrollen im operativen Geschäftsablauf) bis zum [redacted] geplant ist. Die Zertifizierung vom „Typ 2“ wird planmäßig bis zum [redacted] jedes Jahres wiederholt (ON 54).

2.8 Gebühren

Die verfahrensgegenständliche Anzeige beinhaltet grundlegende Änderungen in Bezug auf die Prozesse zur Identitätsprüfung und zur Signaturerstellung, zu denen ein Gutachten in Bezug auf die Sicherheit erstellt wurde.

3. Beweiswürdigung

Die Feststellungen beruhen auf den in Klammern angegebenen Beweismitteln, insbesondere auf dem schlüssigen und nachvollziehbaren Gutachten der nichtamtlichen Sachverständigen (ON 50), dem Schreiben an A-Trust (ON 43), der Stellungnahme von A-Trust zum Gutachten (ON 54), dem Artikel [redacted] (ON 57a), dem Protokoll der Telefonkonferenz (ON 64) und der diesbezüglichen Stellungnahme von A-Trust (ON 66).

4. Rechtliche Beurteilung

4.1 Auflagen zur Mängelbehebung

Im Gutachten der Sachverständigen (ON 50) wurden verschiedene Mängel identifiziert. § 14 Abs 3 SigG ermächtigt die Aufsichtsstelle, einem ZDA die Ausübung seiner Tätigkeit ganz oder teilweise zu untersagen, wenn die für die Ausübung einer solchen Tätigkeit erforderlichen Voraussetzungen nach dem SigG oder den auf seiner Grundlage ergangenen Verordnungen nicht erfüllt werden, sofern nicht nach § 14 Abs 6 SigG gelindere Mittel in Betracht kommen. Gemäß § 14 Abs 6 SigG ist von einer beabsichtigten Untersagung der Tätigkeit abzusehen, soweit die Anordnung gelinderer Mittel – wie Auflagen oder Androhung von Maßnahmen unter Setzung einer angemessenen Frist zur Behebung aufgezeigter Mängel – ausreicht, um die Einhaltung der Bestimmungen des SigG und der SigV 2008 sicherzustellen.

Die noch bestehenden Mängel und die daraus resultierenden Auflagen werden im Folgenden unter Punkt 4.1.1 bis 4.1.7 näher erörtert.

4.1.1 Systembeschreibung für das System der Handy-Signatur und seiner Schnittstellen

Die Auflage, eine finale, in sich konsistente und dem aktuellen Stand der Entwicklung entsprechende Systembeschreibung für das System der Handy-Signatur und seiner Schnittstellen zu erstellen und der Aufsichtsstelle zu übermitteln, soll gewährleisten, dass die für die Handy-Signatur maßgeblichen Einzeldokumente in einem Dokument zusammengeführt werden, um das festgestellte Auftreten von Widersprüchen zwischen den für die jeweiligen Dienste maßgeblichen Sicherheitskonzepten zu vermeiden (Pkt 2.1 der Feststellungen). Die Auflage ist erforderlich, da ein ZDA gemäß § 6 Abs 4 SigG die im Sicherheits- und Zertifizierungskonzept dargelegten Angaben sowohl bei der Aufnahme als auch während der Ausübung seiner Tätigkeit zu erfüllen hat und dies bei Widersprüchen im Sicherheits- und Zertifizierungskonzept nicht möglich ist.

4.1.2 Einsatz von Übertragungsprotokollen

Die Auflage, dass A-Trust das auf der Verbindung zwischen mobilem Endgerät und HSM-Server eingesetzte Protokoll TLS 1.0 bis 30.06.2017 zu deaktivieren und nur noch Protokollversionen ab TLS 1.1 oder neuer einzusetzen hat, beruht auf der glaubwürdigen Feststellung (Pkt 2.2 der Feststellungen), dass TLS 1.0 nicht länger als ausreichend sicher anzusehen ist. Die Auflage ist notwendig, da ein ZDA, der qualifizierte Zertifikate ausstellt, gemäß § 7 Abs 2 SigG für die Signatur- und Zertifizierungsdienste sowie für die Erstellung und Speicherung von Zertifikaten vertrauenswürdige Systeme, Produkte und Verfahren, die vor Veränderungen geschützt sind und für die technische und kryptographische Sicherheit sorgen, zu verwenden hat; bei einem Einsatz der vorerwähnten Protokolle über die Auslauffristen hinaus ist diese Sicherheit nicht länger gewährleistet. Für TLS 1.0 musste die Auslauffrist mit 30.06.2017 deshalb gewählt werden, da noch eine große Anzahl von Kunden diese Protokollversion benötigt, A-Trust jedoch mitgeteilt hat (ON 66, vgl Pkt 2.2. der Feststellungen), dass die Unterstützung für angreifbare kryptographische Algorithmen wie zB RC4 bereits deaktiviert worden sei, und angekündigt hat, dass versucht werde, TLS 1.0 bis Jahresende 2016 gänzlich zu deaktivieren.

4.1.3 Diffie-Hellman-Verfahren

Die Auflage, dass die Implementierung des Diffie-Hellman-Verfahrens dahingehend anzupassen ist, dass [redacted], ist erforderlich, damit der [redacted] Angriff nicht durchgeführt werden kann (vgl Pkt 2.3 der Feststellungen). Die erfolgreiche Durchführung dieses Angriffs würde die Integrität der Handy-Signatur-App so sehr beeinträchtigen, dass sie entgegen § 18 Abs 1 SigG die Fälschung von Signaturen sowie die Verfälschung signierter Daten nicht zuverlässig erkennbar machen und die die unbefugte Verwendung von Signaturerstellungsdaten nicht verlässlich verhindern könnte.

4.1.4 Externe Überprüfung der Handy-Signatur-App

Die Auflage, eine externe Überprüfung der Handy-Signatur-App durchzuführen, ist erforderlich, um zu gewährleisten, dass der Code nicht fehlerhaft ist und keine bewusst undokumentierten Funktionen (Backdoors) enthält (vgl Pkt 2.4 der Feststellungen). Solche Fehler oder undokumentierte Funktionen könnten die Integrität der Handy-Signatur-App so sehr beeinträchtigen, dass sie entgegen § 18 Abs 1 SigG die Fälschung von Signaturen sowie die Verfälschung signierter Daten nicht zuverlässig erkennbar machen und die die

unbefugte Verwendung von Signaturerstellungsdaten nicht verlässlich verhindern könnte. Die Auflage, dass Vorschläge für eine externe Überprüfung bis 30.04.2016 der Aufsichtsstelle zu übermitteln sind, ermöglicht ein Eingreifen der Aufsichtsstelle, falls die von A-Trust ins Auge gefasste Methodik der externen Überprüfung unzureichend ist. Die Auflage, dass das Ergebnis der Überprüfung bis 30.09.2016 zu übermitteln ist, gewährleistet, dass die Aufsichtsstelle von etwaigen Mängeln, die bei der Überprüfung festgestellt werden, Kenntnis erlangt, und räumt A-Trust ausreichend Zeit zur Umsetzung ein (vgl Pkt 2.4 der Feststellungen).

4.1.5 Sicherheitsinformation auf Website

Die Auflage, dass A-Trust auf ihrer Webseite Tipps und Empfehlungen zum Absichern mobiler Endgeräte durch Hinweise auf aktuelle Gefährdungen und Angabe von Virenscannern für jene Betriebssysteme, die dies unterstützen (Android, BlackBerry, Windows Phone) bekannt zu geben hat, ist erforderlich, um Nutzer darüber hinaus auch über aktuelle Gefährdungen der Integrität der Handy-Signatur-App und diesbezügliche vorbeugende Maßnahmen zu informieren, und beruht auf § 4 Abs 2 SigV 2008, wonach eingegebene Autorisierungscodes nicht über den Signaturvorgang hinaus im Speicher verbleiben dürfen und das unbefugte Erfahren dieser Codes durch die Gestaltung des Signaturvorgangs und durch Sperrmechanismen wirksam ausgeschlossen sein muss, wozu die für die Signatoren bereitgestellten Informationen beitragen.

4.1.6 [redacted] – Prozesse bei der Identitätsprüfung

Aufgrund von Pkt 2.6 der Feststellungen sind für Registrierungsverfahren, bei denen eine Identifikation mittels [redacted] erfolgt, verschiedene Prozesse im Zusammenhang mit der Identitätsprüfung zu implementieren. Die in Spruchpkt 1.6 angeführten Auflagen sind erforderlich, um dem in Pkt 2.6 festgestellten Sachverhalt Rechnung zu tragen und die in § 7 Abs 1 Z 4 SigG, § 8 Abs 1 SigG und § 8 Abs 1 SigV 2008 enthaltenen Anforderungen an die Identitätsprüfung von Zertifikatswerbern zu erfüllen.

4.1.7 [redacted] – Beurteilung der Gleichwertigkeit von Videoident-Verfahren

Der in § 8 Abs 1 Z 2 SigV 2008 geforderte Nachweis, der bescheinigt, dass die Identität zumindest mit jener Verlässlichkeit geprüft wurde, wie sie bei der Zustellung zu eigenen Handen einzuhalten ist, kann nach Pkt 2.7 der Feststellungen durch Verwendung des [redacted]-Verfahrens aus heutiger Sicht erbracht werden. Die Auflage, dass A-Trust zu veranlassen hat, dass eine Beurteilung der Vertrauenswürdigkeit von [redacted] im Rahmen der Konformitätsbewertung durch eine Konformitätsbewertungsstelle bis spätestens 01.07.2017 insbesondere hinsichtlich der Sicherheit gegen spezifische Angriffe mittels bild-/video-technischer Bearbeitungsmaßnahmen, hinsichtlich der Anforderungen an Kameraqualität und Lichtverhältnisse für eine zuverlässige Prüfung der frei sichtbaren Sicherheitsmerkmale, hinsichtlich zusätzlicher Angriffsvektoren aufgrund der Verwendung video-basierter Komponenten und hinsichtlich etwaiger Mängel, die sich im Zuge der Zertifizierung oder Rezertifizierung der [redacted] nach ISAE 3402 ergeben haben, erfolgt, ist jedoch im Hinblick darauf erforderlich, dass der Stand der Technik in Bezug auf die Verwendung von Videoidentverfahren im Rahmen der Identitätsprüfung nach den Feststellungen durch die Ergebnisse von Forschungsprojekten wie jenem des BSI beeinflusst werden kann und eine Neubewertung der Eignung dieser Verfahren zur Identitätsprüfung erforderlich machen kann. Die diesbezügliche Frist ergibt sich daraus, dass der ZDA aufgrund von Art 51 Abs 3 VO(EU) Nr. 910/2014 („eIDAS-VO“), ABl L 257/73 vom 28.8.2014, idF ABl L 23/19 vom 29.1.2015 der Aufsichtsstelle ohnehin spätestens bis zum 1.07.2017 einen Konformitätsbewertungsbericht vorzulegen hat, und ist insoweit auch verhältnismäßig.

4.2 Gebühren

Die Anzeige umfasst grundlegende Änderungen der Prozesse zur Signaturerstellung und zur Identitätsprüfung. Durch die Implementierung der Handy-Signatur-App muss sichergestellt werden, dass ein Missbrauch ausgeschlossen ist. Bei der Identitätsprüfung mittels [redacted] muss sichergestellt sein, dass diese zumindest mit der Verlässlichkeit einer Zustellung zu eigenen Handen erfolgt. Beide Prozesse berühren in hohem Maße die Sicherheit der von A-Trust erbrachten Signatur- und Zertifizierungsdienste erbrachten Dienste, weshalb die Änderung des Sicherheits- und Zertifizierungskonzepts der A-Trust als sicherheitsrelevant einzustufen und die Gebühr nach § 1 Abs 1 Z 3 lit b SigV 2008 mit 3.000 Euro zu bestimmen war.

III. Rechtsmittelbelehrung

Gegen diesen Bescheid steht den Parteien dieses Verfahrens gemäß Art 130 Abs 1 B-VG das Rechtsmittel der Beschwerde an das Bundesverwaltungsgericht offen, wobei eine Eingabegebühr in der Höhe von Euro 30,- zu entrichten ist (BGBl II 387/2014). Die Beschwerde ist binnen vier Wochen nach Zustellung dieses Bescheides bei der Behörde, die diesen Bescheid erlassen hat, einzubringen.

Telekom-Control-Kommission

Wien, am 21. März 2016

Die Vorsitzende
Dr. Elfriede Solé