

Informationsvermerk über die technischen Merkmale des von der PRADER BANK AG bereitgestellten Systems für die Verwendung fortgeschrittener elektronischer Signaturen

(gemäß Art. 57, Buchstabe e) der „Technischen Vorschriften für die Erzeugung, das Einfügen und die Überprüfung fortgeschrittener, qualifizierter und digitaler elektronischer Signaturen“, veröffentlicht im Amtsblatt Nr. 117 vom 21. Mai 2013, zur Umsetzung des Kodex für die digitale Verwaltung gemäß dem Gesetzesdekret Nr. 82 vom 7. März 2005 in seiner geänderten Fassung)

Einführung. Zweck des Dokuments und des Glossars.

Der Zweck dieses Dokuments (im Folgenden „Informationsvermerk“) besteht gemäß Artikel 57 Absatz 1 des Dekrets des Präsidenten des Ministerrates (DPCM) vom 22. Februar 2013 in der Offenlegung folgender Informationen:

- die Merkmale des Systems, über das das Unternehmen den elektronischen Signaturdienst bereitstellt;
- die Merkmale der zur Bereitstellung des Dienstes verwendeten Technologien und die Art und Weise, wie sie die Einhaltung der Bestimmungen der geltenden Gesetzgebung ermöglichen;
- die Methoden, über die Kunden Informationen anfordern und eine Kopie der Einwilligung anfordern können;
- die Methoden zur Kontaktaufnahme mit dem Kundendienst.

Das mit dem *fortgeschrittenen elektronischen Signatursystem* (im Folgenden „FES“ genannt) verbundene Verfahren garantiert:

- die Identität des Unterzeichners;
- die eindeutige Verbindung der Signatur mit dem Unterzeichner;
- die ausschließliche Kontrolle des Unterzeichners über das Signaturerstellungssystem;
- die Möglichkeit, zu überprüfen, ob das unterzeichnete Dokument seit der Unterschrift nicht verändert wurde;
- die Möglichkeit für den Unterzeichner, einen Nachweis darüber zu erhalten, was unterzeichnet wurde;
- die Identifizierung des Vermittlers (PRADER BANK AG – im Folgenden auch nur „Bank“), der den Dienst der *fortgeschrittenen elektronischen Signatur* bereitstellt;
- das Fehlen jeglicher Bestandteile des Signaturgegenstandes, die geeignet sind, die in der Signatur dargestellten Handlungen, Tatsachen oder Daten zu verändern;
- die eindeutige Verbindung der Signatur mit dem signierten Dokument;
- das von der Bank implementierte fortgeschrittene elektronische Signaturverfahren, das die folgenden Methoden erfasst:
 - Unterschrift unter Verwendung digitaler Zertifikate, die von der Bank ausgestellt wurden.

Neben der Bank, die als FES-Dienstleister fungiert, sind die folgenden Parteien an dem Prozess beteiligt:

- Daxtor S.r.l., die den Dienst der fortgeschrittenen elektronischen Signatur (FES) anbietet;
- Andxor Srl, die die OTP-Signaturzertifikate bereitstellt.

1. Beschreibung der Merkmale des Systems, das die Identifizierung des Unterzeichners gewährleistet.

- FES mit digitalen Zertifikaten – Die Bank identifiziert ihre Kunden, die die Dokumente unterzeichnen werden, und fordert das entsprechende gültige Ausweisdokument an.

2. Beschreibung der Eigenschaften des Systems, das die eindeutige Zuordnung der Signatur zum Unterzeichner gewährleistet.

Bevor er seine Unterschrift leistet, kann der Unterzeichner das gesamte elektronische Dokument einsehen und seinen Inhalt direkt am Bildschirm überprüfen und validieren. Dieses elektronische Dokument hat die gleichen Eigenschaften wie die früheren Papierversionen, ist jedoch einfacher und effektiver zu verwalten.

- FES mit digitalen Zertifikaten – Diese Methode kann nach der Authentifizierung auf dem Bankportal mit direkt vom Benutzer verwalteter Benutzer-ID und Passwort verwendet werden. Nach der Authentifizierung kann der Benutzer seine PDF-Dokumente im Einzelmodus, über die sichere Web2Sign-Anzeigeplattform oder im Massenmodus direkt über die Dokumentensuchoberfläche

anzeigen, einsehen, durchsuchen und signieren. Die *fortgeschrittene elektronische Signatur* wird auf PDF-Dokumente angewendet, die im sicheren Modus immer über die **Web2Sign**-Plattform angezeigt werden. Insbesondere kann der Kunde elektronische Signaturen nur auf den bereits für die elektronische Signatur des Kunden vorbereiteten Feldern leisten.

Der Kunde kann nur dann unterschreiben, wenn er über ein digitales Zertifikat verfügt, das ihm zuvor von der Bank ausgestellt wurde. Die Anmeldedaten für die Verwendung des besagten Zertifikats müssen sich von den Zugangsdaten zum Portal der PRADER BANK AG unterscheiden, und der Beginn der Unterzeichnungsaktivitäten erfolgt nach der Eingabe von zwei Codes, einem statischen oder PIN, den der Kunde während der Ausstellungsphase des Zertifikats erhält, und dem zweiten dynamischen OTP, der per SMS oder E-Mail empfangen oder über eine spezielle App für Mobiltelefone generiert werden kann, wodurch eine starke und sichere Zwei-Faktor-Authentifizierung gewährleistet wird.

3. Beschreibung der Eigenschaften des Systems, das die ausschließliche Kontrolle des Unterzeichners über das Signaturerstellungssystem gewährleistet.

Während der Unterzeichnungsphase steht das System unter der ausschließlichen Kontrolle des Unterzeichners. Auf dem Bildschirm des Signaturgeräts wird das vollständige Dokument angezeigt, sodass der Unterzeichner seine Daten und alle Vertragsdetails durch Scrollen persönlich überprüfen kann.

- FES mit digitalem Zertifikat - Während des Signierens zeigt der Bildschirm den Inhalt des PDF-Dokuments an. Im Falle des Signierens eines einzelnen Dokuments ist es möglich, mehrere zu signierende Dokumente auszuwählen und mit den Signiervorgängen fortzufahren, nachdem die Klauseln vor dem Signieren angesehen oder akzeptiert wurden. Der Alias des Unterzeichners wird von der Anwendung voreingestellt. Der Benutzer muss zum Zeitpunkt der Unterzeichnung die PIN und das OTP eingeben und seine Absicht zum Ausdruck bringen, mit der Unterzeichnung fortzufahren. Alle diese Aktivitäten werden mit Datum und Uhrzeit im Anwendungsprotokoll festgehalten. Bei der erstellten Signatur handelt es sich um eine Signatur vom Typ PADES, wie sie in europäischen Standards definiert ist.

4. Beschreibung der Merkmale des Systems, die gewährleisten, dass das signierte Computerdokument seit der Signatur nicht verändert wurde.

Die verwendeten elektronischen Signaturtechnologien umfassen Computer-Fingerabdrücke (so genannte „Hashes“) des signierten Inhalts. Die Überprüfung der Übereinstimmung zwischen einem neu berechneten Fingerabdruck und dem „versiegelten“ Fingerabdruck in den Signaturen ermöglicht es, zu überprüfen, ob das signierte Computerdokument seit der Signatur nicht verändert wurde. Im Allgemeinen wird nach Abschluss der Signiervorgänge eine sofortige Überprüfung der Signatur durchgeführt, um die Richtigkeit der Vorgänge zu bestätigen, und alle Dokumente werden anschließend in eine Ersatzablage gebracht.

5. Beschreibung der Merkmale des Systems, das dem Unterzeichner die Möglichkeit gibt, einen Nachweis über die Unterschrift zu erhalten.

Bei der Vorlage des Dokuments zur Unterschrift kann der Unterzeichner den Inhalt in allen Teilen mit spezifischen Positionierungs- und Zoomfunktionen betrachten. Die Eigenschaften des Systems der *fortgeschrittenen elektronischen Signatur* werden entsprechend ausgewählt, um die beste Lesbarkeit zu gewährleisten.

Anschließend hat der Unterzeichner die Möglichkeit, das elektronische Dokument in den mit der Bank gegebenenfalls vereinbarten Formen mithilfe eines ihm vollständig zur Verfügung stehenden Standard-IT-Tools auf einem dauerhaften Datenträger einzusehen, der die Speicherung des Dokuments ermöglicht und er kann es jederzeit ausdrucken (z. B. mithilfe der kostenlosen Software PDF-Reader).

6. Beschreibung der Merkmale des Systems, das dem Unterzeichner die Möglichkeit gibt, einen Nachweis über die Unterschrift zu erhalten.

Das Signaturzertifikat der *fortgeschrittenen elektronischen Signatur* identifiziert den Dienstanbieter und wird von einer technischen Zertifizierungsstelle ausgestellt, die auf die PRADER BANK AG zurückgeführt werden kann und die Bezeichnung „PRADER BANK AG“ trägt. („Details zum Zertifikat“).

7. Beschreibung der Merkmale des Systems, die gewährleisten, dass das Signaturobjekt keine

Elemente enthält, die die darin dargestellten Handlungen, Tatsachen und Daten verändern können.

Die vom System erstellten Dokumente verwenden ausschließlich Formate, die sicherstellen sollen, dass im Gegenstand der Signatur keinerlei Elemente vorhanden sind, die die darin dargestellten Dokumente, Fakten und Daten verändern könnten (ISO-Standardformat PDF/A).

8. Beschreibung der Eigenschaften des Systems, das die eindeutige Verbindung der Signatur mit dem signierten Dokument gewährleistet.

Die Signaturdaten werden in einer Struktur namens „graphometrischer Vektor“ in das Dokument eingefügt, die sie untrennbar mit dem IT-Abdruck des signierten Dokuments verbindet.

Die Anzeige der Signatur, d. h. die Verifizierungsphase, zeigt die Daten im Zertifikat, die auf die natürliche Person zurückgeführt werden können, die den Signiervorgang nach einer starken Authentifizierung durchgeführt hat, die nur auf den Inhaber des Zertifikats zurückgeführt werden kann.

9. Beschreibung der Merkmale der Technologien, die im Dienst für fortgeschrittene elektronische Signaturen eingesetzt werden, um die unter den Nummern 1 bis 8 genannten Anforderungen zu erfüllen.

Die Übertragung der Daten und deren Speicherung im „graphometrischen Vektor“ wird durch folgende kryptografische Technologien geschützt:

- RSA 2048 Bit mit privatem Schlüssel, der von einem Dritten für die AES-Schlüsselverschlüsselung gehalten wird.
Die Verschlüsselung ist asymmetrisch und wird daher mit einem Paar RSA 2048-Schlüssel/Zertifikat durchgeführt, das von einer bei AGID registrierten CA ausgestellt wird. Insbesondere wird der öffentliche Teil (Zertifikat) für die Verschlüsselung der Daten verwendet, während die Entschlüsselung der Daten nur mit Zugang zum entsprechenden privaten Schlüssel erfolgen kann, der in der Regel in einem sicheren, normgerechten Gerät, einem HSM oder auf einer Smart Card aufbewahrt wird, die in einem Schließfach der Einrichtung selbst, eines Notars oder einer Zertifizierungsstelle aufbewahrt wird, wodurch im Falle eines Rechtsstreits der ausschließliche Zugang zu den Nutzern gewährleistet ist, die das Recht dazu haben (Beamte/Justiz);
- Elektronische Signatur mit PDF-Dokumentenzertifikat, durchgeführt mit PADES-Signatur (Standard und wie bei der digitalen Signatur).

10. Beschreibung der Mittel, mit denen die Kunden eine kostenlose Kopie des von ihnen unterzeichneten Antragsformulars für den fortgeschrittenen elektronischen Signaturdienst anfordern können.

Die Kunden können bei der Bank kostenlos einen Ausdruck des Formulars für den Zugang zum Dienst der *fortgeschrittenen elektronischen Signatur* sowie der auf diese Weise unterzeichneten Bank- und Finanzdokumente und -urkunden anfordern.

11. Beschreibung der Mittel, mit denen die Kunden die unter den Punkten 1. bis 8. genannten Informationen anfordern können.

Dieses Dokument, das Informationen über die Merkmale des Dienstes der *fortgeschrittenen elektronischen Signatur* und die ihm zugrunde liegenden Technologien enthält, wird gut sichtbar auf der Startseite der Website www.praderbank.com veröffentlicht und ist somit für Kunden und die breite Öffentlichkeit jederzeit zugänglich. Für weitere Informationen besteht jedoch die Möglichkeit, sich direkt an die Bank zu wenden.

12. Beschreibung des Versicherungsschutzes, den die Bank für die zivilrechtliche Haftung für Schäden an Dritten in Höhe von mindestens 500.000 Euro abschließen muss.

Die Bank hat, gemäß den geltenden Rechtsvorschriften, eine von einer Erstversicherungsgesellschaft ausgestellte Versicherungspolice für die zivilrechtliche Haftung für Schäden an Dritten abgeschlossen, die möglicherweise aus der Bereitstellung des Dienstes der fortgeschrittenen elektronischen Signatur entstehen.