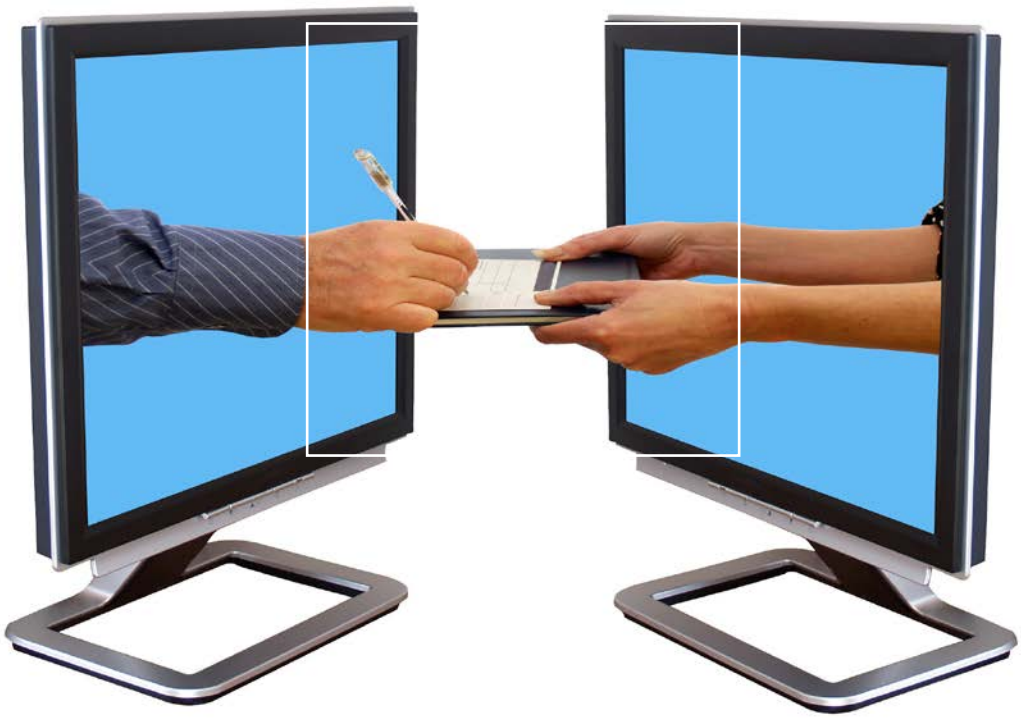
Arthur D Little

Telekommunikation, Information,
Medien & Elektronik

Digitale Signaturen

Auf dem Weg zu einem digitalen Europa



Inhalt

Autoren:

Nicolai Schaettgen
Principal
TIME, Austria
schaettgen.nicolai@adlittle.com

Didier Levy
Director
TIME, France
levy.didier@adlittle.com

Julien Duvaud-Schelnast
Manager
TIME, France
duvaud-schelnast.julien@adlittle.com

Sorana Socol
Business Analyst
TIME, Austria
socol.sorana@adlittle.com

Einleitung

Lösungen für digitale Signaturen ersetzen schnell papier-basierte Unterschriften und haben das Potenzial, signatur-bezogene Prozesse zu dominieren. Die hauptsächlichen Vorzüge dieser Technologie schließen eine gesteigerte Effizienz, geringere Kosten und höhere Kundenzufriedenheit ein.

Prozesse, die noch immer eine handgeschriebene Unterschrift benötigen, verzögern die Wirtschaftlichkeit, steigern die Komplexität durch Archivierung und belasten die Umwelt durch die Nutzung von Papier. Unternehmen neigen aus diesen Gründen verstärkt dazu, sich mit digitalen Unterschriften zu befassen.

Die Finanzbranche hat sich als erste der Entwicklung und Anwendung von Lösungen für Digitale Signaturen zugewendet. Andere, wie etwa Telekommunikation, Handel, Versorgung, Notariate oder das Gesundheitswesen, werden schnell folgen, weil die Vorzüge dieser neuen Technologie – insbesondere höhere Effizienz, geringere Kosten und größere Kundenzufriedenheit - nicht auf bestimmte Branchen limitiert sind. Obwohl Lösungen für Digitale Signaturen klare Vorteile bieten, müssen sie dennoch einige Herausforderungen bewältigen. Dazu gehören die Anpassung der bestehenden Systeme und Prozesse an die neue Technologie, Bedenken hinsichtlich der Akzeptanz durch Geschäftspartner und die vermeintlich hohen Kosten.

Die Europäische Union hat die Regulierung N°910/2014 beschlossen, die den gesetzlichen Wert fortgeschrittener elektronischer Signaturen und entsprechender Services durch die Nutzung eines Systems zur Erzeugung einer qualifizierten digitalen Unterschrift steigert. Diese Regulierung ist im Juli 2014 in Kraft getreten. Diese Entwicklung dient als Beispiel für andere Märkte, wie das Thema der Digitalen Signaturen vom Standpunkt der Rechtsprechung aus angegangen werden kann.

Dieser Report basiert auf einer Befragung von 50 Marktexperten in Europa durch Arthur D. Little sowie einer umfassenden begleitenden Marktanalyse. Der Bericht beinhaltet einen Überblick über die Technologie der Digitalen Signatur, das gegenwärtige und zukünftige Marktpotential sowie die Vorteile und Herausforderungen, die damit verbunden sind. Verschiedene Beispiele für praktische Anwendungen der Digitalen Signatur werden vorgestellt.

.

Digitale Signaturen

Authentizität und Datenintegrität bieten ein hohes Maß an Sicherheit

Lösungen für Digitale Signaturen ersetzen zunehmend papierbasierte Unterschriften und haben das Potenzial, signaturbezogene Prozesse zu dominieren. Die hauptsächlichen Vorzüge dieser Technologie schließen erhöhte Effizienz, geringere Kosten und größere Kundenzufriedenheit ein. Digitale Signaturen müssen klar von gewöhnlichen Authentifizierungsprozessen unterschieden werden. Während Authentifizierung lediglich dazu genutzt wird, die Identität des Endanwenders zu verifizieren, gewährleisten Digitale Signaturen gleichermaßen die Integrität der Daten. Eine Kombination dieser beiden Sicherheitsfaktoren ist für viele Geschäftstransaktionen entscheidend, insbesondere für solche, die sensitive und vertrauliche Daten betreffen.

Digitale Signaturen sind eine Sub-Kategorie elektronischer Signaturen. Während eine Digitale Signatur jede Art von Datum, das einem Dokument hinzugefügt wird, sein kann, wie etwa ein geschriebener Name unter einer E-Mail, basiert eine digitale Signatur auf einem mathematischen Prozess zum Schutz des Dokumentes. Es gibt zwei verschiedene Typen Digitaler Signaturen, die sich lediglich dadurch unterscheiden, wie sicher die Authentifizierung hergestellt wird:

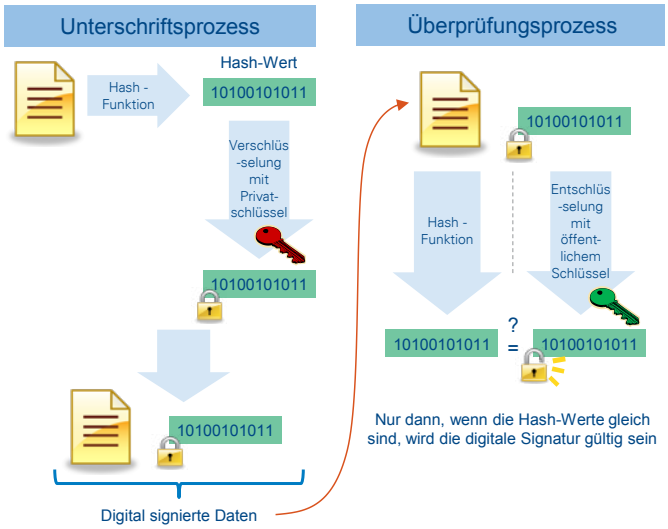
- **Qualifizierte Elektronische Signatur (QES)** ist eine Signatur, die mittels eines anderen sicheren Gerätes erzeugt wird als dasjenige, worauf das Dokument selbst unterschrieben wird. Dies erzeugt eine sehr hohe Sicherheit;
- **Fortgeschrittene Elektronische Signatur (FES)** ist eine Digitale Signatur, die auf dem gleichen Gerät erzeugt werden kann, das auch zur Unterschrift des Dokumentes genutzt wird. Diese Lösung ist weniger sicher als QES.

Eine digitale Signatur schließt drei Prozesse ein: den Unterschriftsprozess, den Authentifizierungsprozess sowie den Prozess zur Sicherstellung der Datenintegrität. Der Prozess zur Erzeugung der digitalen Signatur ist der gleiche, unabhängig davon, ob er intern oder extern stattfindet.

- Der *Unterschriftsprozess* beginnt mit der Bereitstellung eines Dokumentes an den Endanwendern, das von ihm unterschrieben werden muss. Um sicherzugehen, dass die richtige Person das Dokument unterschreibt, wird die Identität des Endanwenders durch eine aus mehreren Faktoren bestehende Authentifizierung verifiziert, wie etwa PIN, Passwort oder sequenz-basierte Token-Codes. Sobald die Identität verifiziert ist, erhält der Unterschreibende ein Zertifikat mit seiner Identität und einem Schlüsselpaar: einem privaten Schlüssel (der nur dem Unterschreibenden bekannt ist) und einem öffentlichen Schlüssel (der öffentlich bekannt ist). Diese Schlüssel sind notwendig, um das Dokument zu signieren und die Identität zu garantieren. Sobald das Zertifikat herausgegeben ist, wird ein einzigartiger mathematischer Code aus dem Dokument generiert. Dieser mathematische Code wird mit dem privaten Schlüssel verschlüsselt (Signieren) und kann nur mit dem korrespondierenden öffentlichen Schlüssel entschlüsselt werden (Verifikation der Signatur). Das Dokument wird anschließend zusammen mit dem verschlüsselten mathematischen Code an den Empfänger gesandt.
- Um die *Authentizität sicherzustellen*, kann der Empfänger mit dem öffentlichen Schlüssel den mathematischen Code entschlüsseln und damit die Authentizität gewährleisten. Der öffentliche Schlüssel funktioniert nur dann, wenn das Dokument mit dem korrespondierenden privaten Schlüssel signiert wurde, der die Identität des Signierenden bereits bestätigt.
- Die *Integrität der Daten* wird durch einen mathematischen Code sichergestellt, der für den Empfänger nach der Entschlüsselung sichtbar wird. Um zu gewährleisten, dass das Dokument nicht durch unberechtigte Personen verändert wurde, kalkuliert der Empfänger seinen eigenen Code aus dem Dokument. Wenn beide Codes übereinstimmen, ist die Integrität der Daten gesichert; wenn das Dokument bei der Übermittlung verändert wurde, würde die Berechnung des Empfängers einen anderen Code ergeben

Bild 1 illustriert den Unterschrifts- und Verifikationsprozess auf Basis der RSA- (Rivest, Shamir und Adleman) Kryptosystem-Technologie, der am weitesten verbreiteten Verschlüsselungstechnologie.

Bild 1: Der Unterschrifts- und Verifikationsprozess der Digitalen Signatur



Quelle: Arthur D. Little

Der beschriebene Verschlüsselungsprozess stellt die Basis für die hohe Sicherheit und die gesetzliche Geltung dieser Technologie dar. Die mathematische Verschlüsselung in Verbindung mit einem hochwertigen Zertifikat sichert die Integrität und die Authentizität der Digitalen Signatur. Die sich daraus ergebende fortgeschrittene Digitale Signatur steht unter EU-Gesetzgebung und ist damit rechtlich wirksam.

Jeder Prozess, der diese Sicherheitsmaßnahmen nicht umfasst, wird als nicht sicher oder gesetzlich wirksam betrachtet. Räumlich entfernte oder persönliche Transaktionen sollten deshalb auf der beschriebenen Prozedur zur Sicherung der Daten beruhen. Beispielsweise ist eine handgeschriebene digitale Unterschrift auf einem Signatur-Pad ohne Digitale Signatur in Gerichtsentscheidungen nicht wirksam – basierend auf einem Gerichtsurteil aus Juni 2012 in Deutschland[1]. Andere gewöhnlich genutzte Techniken schließen etwa die Erkennung biometrischer Daten ein, wie etwa die Geschwindigkeit oder den Druck bei der Unterschrift, um den Unterzeichner zu authentifizieren. Diese Technologie ist sicherer als eine einfache handgeschriebene Unterschrift auf einem Signatur-Pad, wird aber durch EU-Recht und die meisten nationalen Gesetzgebungen nicht unterstützt und bietet deshalb keine rechtliche Sicherheit.

Es bestehen zwei Optionen für Unternehmen, Digitale Signaturen für Endanwender anzubieten: einen extern (durch Drittanbieter) durchgeführten und einen internen (vom Unternehmen selbst) durchgeführten Prozess. Auch wenn beide Vorteile und Nachteile aufweisen, so glaubt Arthur D. Little basierend auf der Analyse von Markttrends, dass der extern durchgeführte Prozess die Lösung der Zukunft sein wird.

Externer Prozess (externe Public-Key-Infrastruktur oder PKI)

Im Rahmen des externen Prozesses stellt eine Third-Party die für die Digitale Signatur benötigten Zertifikate bereit. Diese Third-Party ist verantwortlich für die Bereitstellung einmaliger Zertifikate für Angestellte und / oder Kunden des Unternehmens, nachdem diese authentifiziert worden sind. Bei einem vollständig extern durchgeführten Prozess müssen Unternehmen keine Investitionen für Aufbau und Betrieb der Lösung tätigen, was zu geringeren Gesamtkosten der Implementierung führt.

Der externe Service-Provider sollte eine vollständig **cloud-basierte Lösung** anbieten. Der größte Vorzug hierbei ist, dass die Zertifikate nicht auf irgendeinem SSCD (Secure Signature Creation Device oder Token) gespeichert werden, sondern in der Cloud und deshalb auf jedem Gerät genutzt werden können. Weiterhin muss kein spezieller Software-as-a-Service (SaaS) installiert werden, was den Grad an Vertrauen und Komfort für den Kunden steigert. Studien haben gezeigt, dass Kunden, die aufgefordert werden, eine Software für das digitale Unterzeichnen zu installieren, den Prozess häufiger abbrechen. Für Kunden ist Komfort der beste Anreiz. Digitale Signaturen sind ein deutlich einfacherer Weg ein Dokument zu unterschreiben, etwa im Vergleich zum Einstecken einer e-ID-Card in einen PC oder selbst zur traditionellen handgeschriebenen Unterschrift. Die Cloud ermöglicht Unternehmen auch das Angebot von Multi-Kanal-Signaturen (zum Beispiel von zu Hause oder von einem Mobiltelefon). Weil das mobile Signieren von einem Tablet oder Smart-Phone immer populärer wird, entwickelt sich der cloud-basierte Service zur bevorzugten Technologie. Dies wurde auch durch Interviews bestätigt, die Arthur D. Little durchgeführt hat. Ein Studienteilnehmer antwortete dabei: *"Warum sollten wir von unseren Kunden verlangen, ständig einen Token oder Smart-Card-Reader bei sich zu tragen?"*

Es ist wichtig anzumerken, dass dieses Konzept am sinnvollsten ist, wenn die Third-Party **vertrauenswürdig** ist und sich etwa auf der Vertrauensliste der EU befindet. Dies erhöht nicht nur das gesamte Vertrauensniveau, sondern die von einer vertrauenswürdigen Third-Party bereitgestellten Zertifikate sind weltweit anerkannt. Das bedeutet, dass das Root-Zertifikat, ein Zertifikat, das als vertrauenswürdig akzeptiert ist, bereits

1 http://www.justiz.bayern.de/gericht/olg/m/presse/archiv/2012/03561/

in den meisten Browsern und Betriebssystemen installiert ist und es keine Fehlermeldungen gibt wie bei intern aufgesetzten Prozessen.

Mit Cloud-Lösungen kann die Signatur auch mittels SSCD oder Smart-Card ausgeführt werden. Hier kann die Cloud genutzt werden, um digital signierte Dokumente sicher zu archivieren.

Interner Prozess (Interne PKI)

Die für die Digitale Signatur benötigten Zertifikate werden intern durch die Unternehmung erzeugt und bereitgestellt, die diese Lösungen für Mitarbeiter oder Kunden direkt anbietet. Zertifikate sind nicht einmalig, sondern können wiederverwendet werden, weil sie auf besonderen Badges wie Tokens, Smart-Cards usw. gespeichert werden.

Dieses Konzept verlangt nach einer Infrastruktur, die Identitäten und die korrespondierenden Zertifikate sicher verwaltet. Der Prozess der Implementierung einer PKI erfordert ein Investment in Hardware, Software und Training für Mitarbeiter und eignet sich demnach vorzugsweise für größere Organisationen mit entsprechendem Know-how und Ressourcen. Ein wesentlicher Nachteil der internen PKI besteht darin, dass die Zertifikate in den meisten Fällen von Browsern und Betriebssystemen nicht akzeptiert werden, solange das Unternehmen nicht auf der Vertrauensliste der EU geführt wird.

Jedes Unternehmen muss gewichten, welche Lösung am besten passt, abhängig von den verfügbaren Ressourcen und dem notwendigen Maß an Vertrauen und Kontrolle. Tatsächlich gibt es bereits Indizien dafür, dass Lösungen, die zusätzliche externe Geräte benötigen, um Digitale Signaturen zu erzeugen, allgemein nicht besonders populär sind. 15 europäische Länder haben elektronische Ausweise (eID) herausgegeben, die Informationen für die Online-Authentifizierung enthalten, die meisten davon mit einer optionalen Funktion für die Digitale Signatur. Um diese Funktion für die Digitale Signatur nutzen zu können, muss ein Kartenleser für die eID angeschafft werden, was das Konzept weiter kompliziert.

Das Potenzial dieser Lösung könnte allerdings mit NFC (Near Field Communication) verbessert werden, einer Technologie, die die Nutzung der Digitalen Signatur mit eIDs ohne Kartenleser ermöglicht, etwa durch die Nutzung eines NFC-Smartphones. Auch wenn die Möglichkeit zur Unterschrift mittels eines Smartphones ein höheres Maß an Mobilität garantieren würde, so wird dennoch erwartet, dass vollständig cloud-basierte Lösungen ohne Karten und Kartenleser den zukünftigen Markt für Digitale Signaturen dominieren werden, weil das Maß an Komfort einen entscheidenden Faktor für die Auswahl der Lösung darstellt.

Geringe Kosten und größere Effizienz sind wesentliche Vorteile

Digitale Signaturen können in einer Vielzahl von Bereichen eingesetzt werden, da Unternehmen sie für ihre internen Prozesse ebenso nutzen können wie für die Kommunikation mit Geschäftspartnern und Kunden. Behörden sind eine weitere wichtige Kategorie als Kunden für diese Technologie, weil sie zunehmend gefordert sind, schlankere und kostenminimierende Prozesse zu implementieren.

Viele Unternehmen und Behörden haben bereits das Potenzial dieser Technologie erkannt. Ein vollständig digitaler Prozess für die Signierung und den Versand von Dokumenten senkt die Arbeitszeiten und Kosten für Papier und Transport. Die Untersuchung von Arthur D. Little und weitere Analysen bestätigen, dass eine unmittelbare Nutzung der Technologie das Potenzial hat, nachhaltige Wettbewerbsvorteile zu erzielen, unabhängig von der Branche, in der das Unternehmen tätig ist.

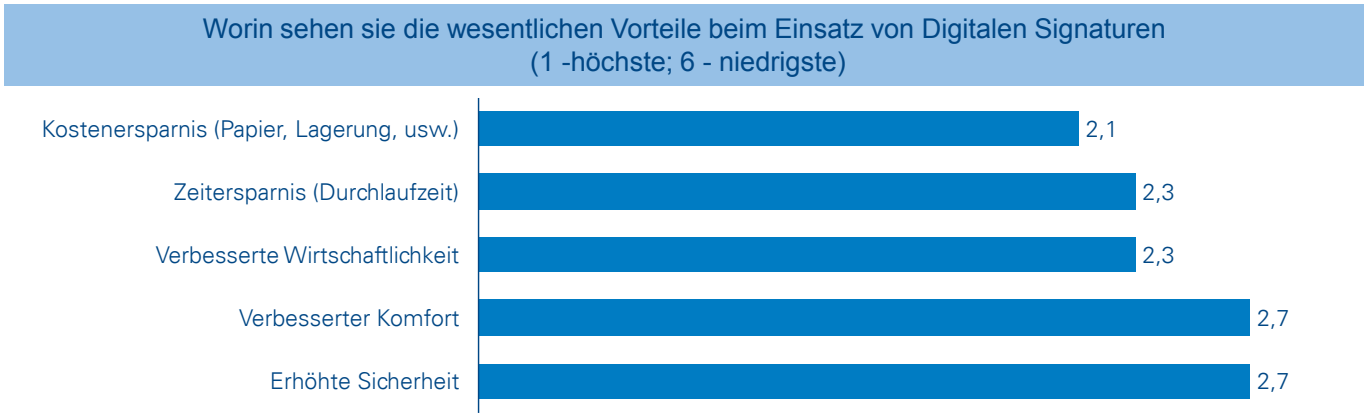
Gemäß den Ergebnissen der Untersuchung von Arthur D. Little ist das tragende Argument für den Einsatz der Technologie eine verbesserte Effizienz, die zur Verringerung der Kosten und der Erhöhung der Geschwindigkeit des gesamten Geschäftes führt. Die Nutzung der Digitalen Signatur senkt den Aufwand durch die Reduktion der Prozesskosten wie Scannen, Aufzeichnen, Archivieren, Drucken und Versenden und reduziert Ressourcenaufwendungen (kürzere Prozesszyklen resultieren in geringeren Personalausgaben). Geschäftsprozesse werden zusätzlich effizienter durch die Verbesserung der allgemeinen Flexibilität von Unternehmen (reduzierte Prozesszyklen, Geschwindigkeit von Geschäftsabschlüssen) und durch die Verfolgung und Koordination der Geschäfte in Echtzeit.

Neben den Effizienzüberlegungen bedeutet die Einführung von Lösungen für Digitale Signaturen ein innovatives Image sowohl für den Nutzer als auch für Anbieter der Technologie. Außerdem erhöhen diese Lösungen die Kundenzufriedenheit. Zum Beispiel können Banken ihren Kunden mehrere unterschiedliche Kanäle anbieten, um eine Kreditvereinbarung zu signieren.

Auch wenn Branchenexperten, die an dem Report teilgenommen haben, eine gesteigerte Sicherheit nicht als Hauptvorzug der Technologie hervorheben, so bieten Digitale Signaturen dennoch ein höheres Maß an Sicherheit gegenüber traditionellen Methoden des Versandes von Dokumenten, sofern sie zusammen mit kryptographischen Prozeduren und qualifizierten Zertifikaten implementiert werden:

- Die Integrität der Daten kann zugesichert werden, weil eine Fälschung praktisch unmöglich ist, während ein Papierdokument nach der Unterschrift durch eine unberechtigte Person modifiziert werden kann.
- Die Wahrscheinlichkeit, eine digitale Kopie zu verlieren, ist wesentlich geringer im Vergleich zu papier-basierten Dokumenten.
- Alle Datentypen wie Fotos oder Audio-Dateien können digital unterschrieben werden, was das Copyright dieser Materialien schützt.
- Ein Zeitstempel kann zu der Digitalen Signatur hinzugefügt werden, der bescheinigt, dass das Dokument an einem bestimmten Datum signiert wurde.

Bild 2: Die Hauptvorteile Digitaler Signaturen



Quelle: Arthur D. Little, Hinweis: Alle Zahlen stellen Durchschnittswerte dar

Mehrere Herausforderungen müssen noch bewältigt werden

Trotz des Potenziales der Technologie bedeutet die Implementierung von Systemen für die Digitale Signatur auch diverse Herausforderungen. Die meisten Unternehmen haben Systeme und Prozesse bezüglich der traditionellen Methoden der Vertragsunterschrift entwickelt. Von den Schreibtischen der Angestellten bis hin zur Archivierung der signierten Dokumente wurde die *Adaption existierender Anwendungen oder Systeme* bei den Interviews als ein Hauptproblem angesehen. Unternehmen und Institutionen, die sich für die Einführung der Technologie interessieren, hängen intensiv von vertrauenswürdigen, einfach zu implementierenden und komfortablen Lösungen ab, die die Komplexität von Arbeitsabläufen nicht erhöhen. Anbieter, die in der Lage sind, diese wichtige Mischung von Charakteristika bereitzustellen, werden über substanzielle Wettbewerbsvorteile im Markt für Digitale Signaturen verfügen.

Zusätzlich besteht nach wie vor das Problem der *Akzeptanz bei Geschäftspartnern und Kunden*. Aus der Untersuchung ergibt sich jedoch klar, dass die Akzeptanz stark von den Lösungen abhängt, die den Kunden angeboten werden. Eine breite Palette an bereits implementierten Lösungen, die eine einfache Nutzung garantieren, wird die Akzeptanz bei Kunden und Geschäftspartnern erhöhen.

Unter den Teilnehmern der Studie gab es zudem den Eindruck, dass die Implementierung von Lösungen für Digitale Signaturen mit *hohen Investitionen* verbunden ist. Dieses Argument kann kurzfristig stichhaltig sein, aber reduzierte Kosten wiegen die Investitionen gewöhnlich in kurzer Zeit auf. Die Kosten für eine bestimmte Lösung hängen vom Typ der Implementierung ab. Cloud-Lösungen führen zu geringeren Implementierungskosten. Die Gesamtkosten hängen allerdings immer vom Preismodell der Lösung und von der Nutzungsfrequenz ab.

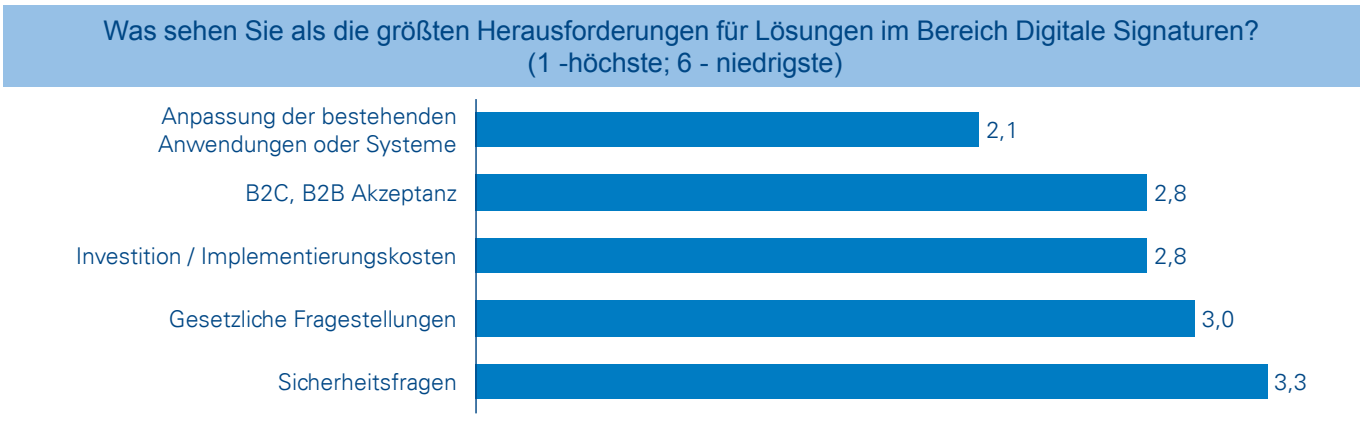
Zertifizierte e-Mails können ein Risiko für Digitale Signaturen darstellen

Zertifizierte e-Mails sind ein Service, der auch darauf abzielt, einen sicheren Datentransfer zwischen Sender und Empfänger zu ermöglichen, indem e-Mails durch den Sender verschlüsselt und durch den Empfänger wieder entschlüsselt werden. Um dies zu erreichen, müssen Sender und Empfänger über einen zertifizierten e-Mail-Account bei einem zertifizierten Provider verfügen sowie über eine Software, die in der Lage ist, e-Mails zu ver- und zu entschlüsseln. Falls die Authentifizierung des Senders in der vorliegenden Transaktion eine wichtige Rolle spielt, kann die zertifizierte e-Mail auch digital unterschrieben werden (mit einer qualifizierten Digitalen Signatur).

Ein größeres Sicherheitsproblem der zertifizierten e-Mails besteht darin, dass sie nicht auf einem durchgängigen Verschlüsselungsprozess beruhen, was bedeutet, dass jede e-Mail die durch den Sender verschlüsselt wurde, durch beide zertifizierte e-Mail-Provider entschlüsselt wird (die e-Mail kann also gelesen und modifiziert werden). Dies bedeutet ein Sicherheitsproblem, das durch unberechtigte Parteien ausgenutzt werden könnte. Es gibt zwar eine Möglichkeit für eine durchgängige Verschlüsselung, diese erfordert aber zusätzliche Verschlüsselungssoftware.

Im Vergleich zu klassischen Lösungen für Digitale Signaturen hat e-Mail Nachteile bei der Sicherheit und beim Komfort, weil das Standard-Modell nicht auf Ende-zu-Ende-Verschlüsselung beruht und sowohl der Sender als auch der Empfänger über einen zertifizierten e-Mail-Account verfügen müssen.

Bild 3: Die wichtigsten Herausforderungen der Digitalen Signaturen



Quelle: Arthur D. Little, Hinweis: Alle Zahlen stellen Durchschnittswerte dar

Die neue Gesetzgebung wird die Nutzung von E-Signaturen weiter beschleunigen

Die Europäische Gesetzgebung basiert im Wesentlichen auf der Richtlinie 1999/93/EC, die gemeinsame Verpflichtungen für Zertifizierungs-Service-Provider festlegt sowie gemeinsame Regeln für die Haftung und kooperative Mechanismen für die grenzüberschreitende Anerkennung von Signaturen und Zertifikaten innerhalb der gesamten Europäischen Gemeinschaft. Die Richtlinie adressiert drei Formen der Digitalen Signatur: einfache, fortgeschrittene und qualifizierte Digitale Signatur.

Die Europäische Union hat die Regulierung N°910/2014 beschlossen, um die Nutzung der Digitalen Identifikation und Signaturen in der gesamten Union zu konsolidieren. Wichtige Eckpunkte der neuen EU-Richtlinie sind die Überwindung bestehender Barrieren für die Bereitstellung eines umfassenden grenz- und branchenüberschreitenden Rahmenwerks für sichere, vertrauenswürdige und einfach anzuwendende elektronische Transaktionen wie auch das Potenzial, Cloud-Signaturen zu ermöglichen, um ein Höchstmaß an Sicherheit zu erreichen. Vollständig cloud-basierte Signaturen werden möglich sein, sobald einige finale Anforderungen erfüllt werden.

Die Interviews, die Arthur D. Little mit Branchenexperten geführt hat, bestätigen den generellen Eindruck, dass das Gesetz zwar klar definiert, aber in der breiten Öffentlichkeit noch nicht transparent ist. Dies schafft Herausforderungen für den Einsatz und das Potenzial der Technologien.

Der Markt für Digitale Signaturen ist hochfragmentiert und dynamisch

Um eine Digitale Signatur zu erstellen, wird eine sichere Umgebung benötigt, die es ermöglicht, die digitalen Zertifikate zu verwalten (Herausgabe, Speicherung und Nutzung). Diese Umgebung wird Public-Key-Infrastruktur (PKI) genannt und kann entweder lokal im Hause durch den Serviceanbieter oder extern durch einen Cloud-Solution-Provider mit Zugang über das Internet verwaltet werden. In beiden Fällen offeriert der Anbieter wie etwa eine Bank den Service an einen End-Anwender. Entweder wird der Token oder ein anderes Gerät, auf dem das Zertifikat gespeichert ist, dem Endanwender übergeben, oder der Anwender muss über die Cloud unterschreiben.

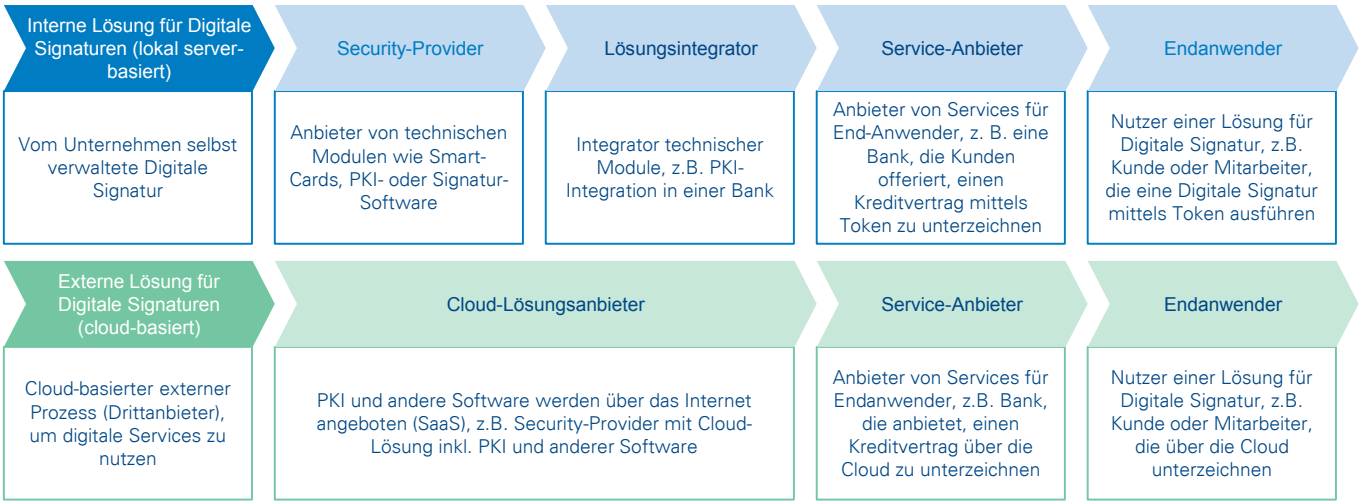
Die an der Implementierung und den Anwendungsphasen von Lösungen für Digitale Signaturen beteiligten Parteien sind im Detail aus der untenstehenden Grafik ersichtlich.

Der Markt für Digitale Signaturen in Europa ist gegenwärtig klein, hochfragmentiert und dynamisch. Es gibt neue Anbieter mit neuen Technologien, etablierte Anbieter, die sich ausschließlich auf den Signatur-Markt konzentrieren sowie Anbieter aus anderen Branchen, die versuchen zu diversifizieren. Anbietern aus Europa, wie OpenTrust oder D-Trust, stehen amerikanische Anbieter gegenüber, die den europäischen Markt bedienen wollen, wie Adobe Echosign, ARX CoSign oder DocuSign, das bereits seit drei Jahren über Büros in UK verfügt. Um ihren Markteintritt in Europa zu ermöglichen, haben einige der US-Player Partnerschaften mit lokalen Anbietern geschlossen. OpenTrust wurde zum europäischen Partner von DocuSign, um gemeinsam eine neue Lösung für die Digitale Signatur zu entwickeln, die einfache Anwendung und die Erfüllung der EU-Richtlinien kombiniert.

Um die Komplexität des Marktes zu unterstreichen und einen Überblick über die wesentlichen Player zu geben, wurden Typologien mittels eines investigativen Bottom-Up-Ansatzes erstellt. Basierend auf den gewählten Typologien wurden fünfzehn der wichtigsten Anbieter von Lösungen für Digitale Signaturen auf dem europäischen Markt untersucht.

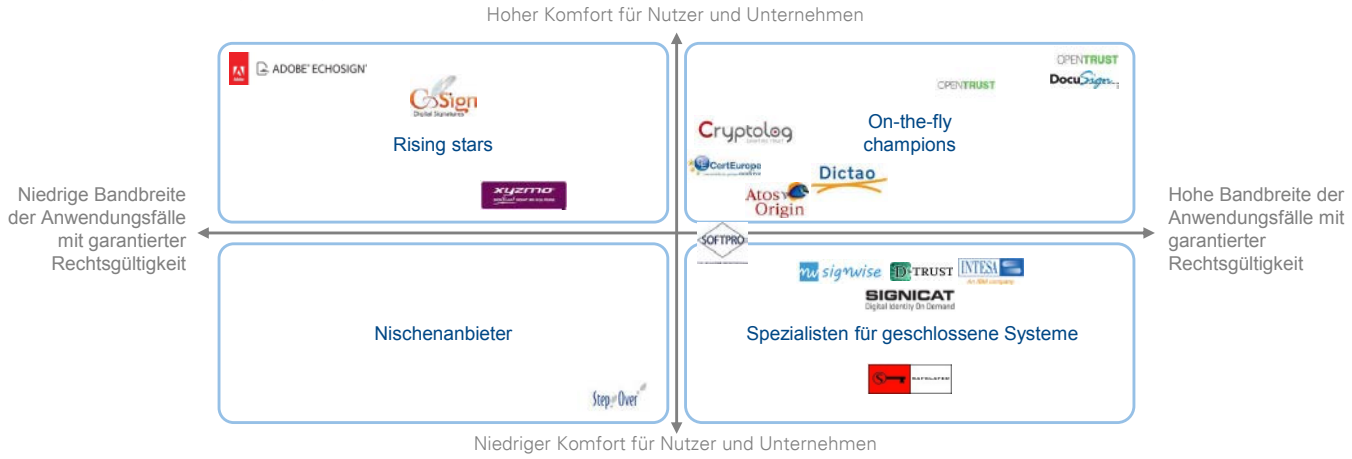
- **Zweckmäßigkeit für Anwender und Unternehmen:** Hoher Komfort bedeutet, dass der Kunde Signaturen von jedem Computer, Tablet oder Smartphone erzeugen kann, dass keine externe Geräte wie Hardware-Token oder e-ID-Card notwendig sind oder dass es keine Notwendigkeit gibt, Software (SaaS) zu installieren. Dieses hohe Maß an Komfort erfordert keine interne PKI, die Archivierung (Evidence Management) erfolgt extern und es muss keine Software installiert werden (SaaS).
- **Anwendungsvielfalt mit gesetzlicher Wirksamkeit:** Eine Vielfalt an Anwendungsfällen, die rechtlich abgesichert sind (unterstützt durch FES oder zumindest AES und basierend auf qualifizierten Zertifikaten) bedeutet, dass die Lösungen für eine Digitale Signatur, die dem Kunden angeboten werden, den Status der Vertrauenswürdigkeit haben.

Bild 4: Die Wertschöpfungskette der Digitalen Signatur



Quelle: Arthur D. Little

Bild 5: Der Markt für Digitale Signaturen



Quelle: Arthur D. Little

Basierend auf den definierten Dimensionen haben wir vier Haupttypologien von Anbietern definiert:

- On-the-fly Champions
- Spezialisten für geschlossene Systeme
- Nischenanbieter
- Rising Stars

On-the-fly Champions sind Anbieter, die hochkomfortable Lösungen für Kunden anbieten, wie etwa Unternehmen des Finanzwesens, Banken oder andere hochregulierte Branchen, die durch die Natur ihrer Arbeit viele Referenzen und Zertifizierungen benötigen, um die Rechtswirksamkeit der Digitalen Signatur zu garantieren. In einem Markt, in dem kundenfreundliche Lösungen (SaaS) der Schlüssel für den Erfolg sind, bieten On-the-fly Champions die beste Adaptierbarkeit an die Kundenanforderungen und verfügen über die höchste Rechtswirksamkeit der angebotenen Lösungen. Der klare Anführer unter den On-the-fly Champions in Europa sowohl für B2C als auch für B2B ist der französische Anbieter OpenTrust, der Erfinder von Offline- und Cloud-Signaturen (Cloud System zertifiziert nach ETSI TS 102 042, ETSI TS 102 023 und TÜV IT). Positioniert als Online-Notar und mit einem Fokus auf die Jurisprudenz, bietet OpenTrust rechtlich wirksame Lösungen für die Digitale Signatur mit hohem Komfort für Anwender und Unternehmen.

Spezialisten für geschlossene Systeme bieten Lösungen, die nicht cloud-basiert sind für mittlere und große Unternehmen mit vielen Kundeninteraktionen und einem breiten Spektrum interner Prozesse, die eine Nutzung der Digitalen Signatur benötigen und die eine interne Verwaltung der Signaturlösungen bevorzugen. Unternehmen, die bereits interne PKI-Systeme betreiben und schon Badges mit Zertifikaten benutzen, können diese weiterverwenden. Allerdings müssen sie das PKI-System verwalten, und die Lösung hängt stark von den Betriebssystemen und den Web-Browsern ab, die sich jeweils weiterentwickeln. Der spanische Player SafeLayer hat eine etablierte Präsenz auf dem europäischen Markt vor allem als Anbieter von digitalen Signaturlösungen für Finanzinstitute und öffentliche Verwaltungen, die aufgrund ihres hohen Niveaus vertraulicher Daten viele rechtlich wirksame Anwendungsfälle benötigen wie auch Lösungen, die auf ihren eigenen Servern basieren, im Gegensatz zu cloud-basierten Lösungen.

Nischenanbieter offerieren interne Lösungen für kleinere Kunden, die nicht viele Anwendungsfälle benötigen bzw. nicht viele Endanwender-Interaktionen unterstützen müssen. Diese Lösungen sind nicht kompatibel mit Multi-Channel- oder Multi-Device-Strategien, was zu einer weniger komfortablen und interaktiven Nutzererfahrung führt. Sie bieten aber den Vorteil des internen Managements der Lösung. Der deutsche Player StepOver ist ein Nischenanbieter, der sowohl Software für die Digitale Signatur als auch Hardwarekomponenten anbietet. Derzeit werden bereits 100.000 StepOver Signatur-Pads genutzt. StepOver ist ein starker Partner von kleineren Unternehmen, die ein internes Management ihrer Lösungen für Digitale Signaturen bevorzugen.

Rising Stars sind kleinere Anbieter cloud-basierter und komfortabler Lösungen mit einer limitierten Anzahl von Anwendungsfällen und ohne EU Rechtswirksamkeit. Sie haben das Potenzial, zu den nächsten On-the-fly Champions zu werden. Allerdings haben sie noch einen weiten Weg vor sich, um zertifiziert zu werden (ETSI 101, 192 etc.), um auf die Liste der EU für vertrauenswürdige Zertifizierungsstellen zu kommen und um eine Kundenbasis aufzubauen. Der US-basierte Anbieter ARX CoSign zum Beispiel ist ein kleinerer Player auf dem europäischen Markt. Mit komfortablen Lösungen ohne EU-Rechtswirksamkeit benötigt CoSign weitere Zertifizierungen, um die rechtliche Gültigkeit der Produkte zu steigern und die Kundenbasis in Europa zu erhöhen.

Konkrete Beispiele bieten Aufschlüsse über die praktische Anwendbarkeit der Digitalen Signatur

Digitale Signaturen können in unterschiedlichsten Arbeitsprozessen in fast jeder Branche zum Einsatz kommen. Anwendungsfälle umfassen verschiedenste Arten von Kommunikation, in der Willenserklärungen kombiniert mit der Authentifizierung der beteiligten Parteien benötigt werden oder gesetzlich vorgeschrieben sind. Über eID-Services hinaus, die gemäß Sekundärrecherchen aufgrund der geringen Zweckmäßigkeit der Gesamtlösung noch nicht sehr erfolgreich sind, gehört der wirkliche Markt bedingt durch den Komfort der Lösungen den cloud-basierten Digitalen Signaturen. Der Kunde kann sich den Vertrag, die Steuererklärung oder Import- und Export-Abgaben auf jedem Gerät ansehen, seien es PCs, Tablets oder Smartphones; er kann eine SMS für die Authentifizierung erhalten und dann ohne die Notwendigkeit für spezielle Hard- oder Software unterschreiben.

Im Rahmen dieses Reports haben wir folgende Segmentierung der Digitalen Signaturen vorgenommen:

- Business-to-Business (B2B)
- Business-to-Customer (B2C)
- Behörden

Die Anwendungsfälle unterscheiden weiterhin zwischen Remote- und Face-to-Face-Transaktionen.

- **Remote:** Der Unterzeichner signiert das Dokument ohne physikalische Präsenz eines Vertreters des Unternehmens, das den Service anbietet, etwa einer Bank. Die Authentifizierung erfolgt ebenso mittels einer Remote-Methode (z.B. Einmal-Passwort, SMS etc.).
- **Face-to-Face:** Der Unterzeichner signiert das Dokument mit physikalischer Anwesenheit eines Vertreters des Unternehmens, das den Service anbietet. Der Repräsentant nimmt ebenso die Authentifizierung des Unterzeichners vor (z.B. mittels Pass oder Personalausweis).

Aufgrund der durchgeführten Interviews, aktueller Projektanfragen und zusätzlicher Recherche hat Arthur D. Little einen steilen Anstieg der Zahl von Unternehmen festgestellt, die bereits zu „Digitalen Unternehmen“ transformieren oder dies planen.

Desweiteren wird beobachtet, dass die Akzeptanz im B2B-Umfeld hoch ist, weil technologisch fortgeschrittene Geschäftspartner als Rollenmodelle dienen.

Verbreitete Anwendungsfälle bei B2B	
Remote	**Face-to-Face**
▪ Internes Management der Dokumente ▪ Verwaltung von Lieferantenverträgen ▪ Verwaltung von Kundenverträgen ▪ Verwaltung von Personalverträgen	▪ Vertragsunterzeichnung mit Außendienst (z.B. Versicherung, Finanzierung)

Die angewandten Nutzungsbeispiele bei B2C hängen stark von der rechtlichen Wirksamkeit und der allgemeinen Kundenakzeptanz dieser Technologien ab, die sich von Markt zu Markt unterscheiden. Zu den Pionieren beim Angebot derartiger Lösungen für Endkunden gehören Zusteller, Banken und Versicherungen.

Häufige Anwendungsfälle bei Behörden	
Remote	**Face-to-Face**
▪ Online-Bestellungen ▪ SEPA SDD Kundenverwaltung ▪ Konteneröffnungen	▪ Vertragsunterzeichnung auf Tablets in Zweigstellen ▪ Vertragsunterzeichnung auf Tablets durch Händler und Distributoren (z.B. Kredite, Versicherungen)

Behörden sind im Allgemeinen die treibenden Kräfte hinter der branchenüberschreitenden Verbreitung der Technologie in Europa. Der Kostendruck nötigt viele Behörden dazu, über schlankere Prozesse nachzudenken und gleichzeitig die Sicherheit für sensitive kommerzielle und personenbezogene Daten zu garantieren. Viele Behörden in Europa bieten den Unternehmen oder Bürgern an – oder verpflichten sie sogar dazu – mit ihnen auf digitalen Wegen zu kommunizieren.

Häufige Anwendungsfälle bei Behörden	
Remote und Face-to-Face	
▪ Online-Bestellungen ▪ SEPA SDD Kundenverwaltung ▪ Konteneröffnungen	▪ Vertragsunterzeichnung auf Tablets in Zweigstellen ▪ Vertragsunterzeichnung auf Tablets durch Händler und Distributoren (z.B. Kredite, Versicherungen)

Beispiel Credit AgricoleConsumer Finance[2]

Das folgende Anwendungsbeispiel Credit Agricole Consumer Finance wurde durch Arthur D. Little in Zusammenarbeit mit OpenTrust, dem Lieferanten der Credit Agricole, erarbeitet. OpenTrust ist ein führender Anbieter von on-the-fly Lösungen für Digitale Signaturen in Europa sowohl für B2B als auch für B2C.

Unternehmensüberblick	▪ Credit Agricole Consumer Finance ist ein führender Anbieter von Konsumentenkrediten in Frankreich und Europa ▪ Produkte: Finanzprodukte und –services (Direktvertrieb, Point-of-Sale-Finanzierung, e-Commerce, Partnerschaften) ▪ In 22 Ländern aktiv
Hauptsächliche Gründe für den Einsatz	▪ Kunden erwarteten die Modernisierung der Arbeitsprozesse und Produkte ▪ Kostenreduktion
Konzept der digitalen Lösung	▪ Betrieb in 22 Ländern
Anwendungsbereiche	▪ Face-to-Face-Transaktionen (B2B in Frankreich, B2C in Italien, andere Länder folgen in den kommenden Jahren) ▪ Keine interne Nutzung bisher (sichere Authentifizierung ist bereits vorhanden) ▪ B2B2C-Transaktionen mit dem Ziel, die Digitale Signatur in die Anwendungen der Credit-Agricole-Partner zu integrieren (z.B. Einbindung der Digitalen Signatur in die Abmeldung bei einer e-Commerce-Website)
Erreichte Vorteile	▪ Erhöhung der Kundenzufriedenheit durch die Wahrnehmung als innovativer Anbieter ▪ Erwartete geringere Kosten in den nächsten Jahren im Verhältnis zum papier-basierten Ansatz („wird sich definitiv in der näheren Zukunft auszahlen“)
Herausforderungen	▪ Notwendige Zeit, um eine gute „Customer-Journey“ zu garantieren (der gesamte Arbeitsprozess – nicht nur die Digitale Signatur – musste angepasst werden ▪ Die Klarstellung der rechtlichen Wirksamkeit benötigte Aufwand (Rechtsberatung notwendig) ▪ Hohe initiale Kosten bei der Anpassung der Prozesse
Wesentliche Kriterien bei der Lieferantenauswahl	▪ Rechtlich wirksame Lösung ▪ Partnerschaftliche Zusammenarbeit ▪ Technische Expertise
Schlüsselüberlegungen bei der Wahl des Anbieters	▪ Rechtliche Wirksamkeit der Lösung, rechtliche Beratung durch den Anbieter möglich ▪ Standardisierte Lösung für europaweiten Einsatz

2 Information gesammelt durch Interview mit Vertreter von Credit Agricole/CA Consumer Finance

Fazit

Die Technologie der Digitalen Signatur wird in vielen Bereichen unseres täglichen Lebens präsent sein, die Vertraulichkeit benötigen. Die Technologie bringt höhere Effizienz und Kosteneinsparungen und wird zunehmend als Kommunikationswerkzeug zwischen Geschäftspartnern, Kunden und öffentlichen Einrichtungen genutzt. Wie immer bei relativ neuen Technologien müssen auch hier Hürden übersprungen werden. Dazu gehören die einfache Integration und das Zusammenspiel mit existierenden Arbeitsprozessen, die Kalkulation des Anwendungsfalles wie auch die mangelnde Transparenz sowie eine häufige Fehleinschätzung der rechtlichen Situation. Mit der neuen EU-Richtlinie, die in 2014 umgesetzt wurde, und die eine umfassende rechtliche Wirksamkeit sowie die Akzeptanz cloud-basierter Lösungen vorantreibt, gibt es bereits sehr vielversprechende Anzeichen, dass die Behörden und die Branche die Herausforderungen überwinden können. Weil der Markt nach einem schnellen Return-on-Investment und Lösungen verlangt, die Arbeitsprozesse vereinfachen, wird erwartet, dass vollständig oder teilweise cloud-basierte Anwendungen der Digitalen Signatur den Markt in der Zukunft beherrschen. Anwender, die das Potenzial derartiger Lösungen heute erkennen, werden in der Lage sein, signifikante Kostenvorteile zu erzielen sowie ihre Kundenbasis besser verwalten und erweitern, weil diese Lösungen einen höheren Komfort bieten.

Kontakt

Für weitere Hintergrundinformationen und Gespräche stehen wir ihnen gerne zur Verfügung:

Austria
Karim Taga
taga.karim@adlittle.com

Belgium
Gregory Pankert
pankert.gregory@adlittle.com

China
Antoine Doyon
doyon.antoine@adlittle.com

Czech Republic
Dean Brabec
brabec.dean@adlittle.com

France
Didier Levy
levy.didier@adlittle.com

Germany
Michael Opitz
opitz.michael@adlittle.com

India
Srini Srinivasan
srinivasan.srini@adlittle.com

Italy
Giancarlo Agresti
agresti.giancarlo@adlittle.com

Japan
Shinichi Akayama
akayama.shinichi@adlittle.com

Korea
Kevin Lee
lee.kevin@adlittle.com

Latin America
Vincenzo Basile
basile.vincenzo@adlittle.com

Middle East / Malaysia
Thomas Kuruvilla
kuruvilla.thomas@adlittle.com

The Netherlands
Martijn Eikelenboom
eikelenboom.martijn@adlittle.com

Nordic
Martin Glaumann
glaumann.martin@adlittle.com

Singapore
Yuma Ito
ito.yuma@adlittle.com

Spain
Jesus Portal
portal.jesus@adlittle.com

Switzerland
Clemens Schwaiger
schwaiger.clemens@adlittle.com

UK
Richard Swinford
swinford.richard@adlittle.com

USA
John Brennan
brennan.john@adlittle.com

Arthur D. Little

Arthur D. Little zählt seit 1886 zu den Innovationsführern in der Consultingbranche. Wir sind ein anerkannter Experte für Unternehmen, die Strategie, Innovation und Transformation in technologieintensiven und konvergierenden Branchen verbinden wollen.

Arthur D. Little navigiert Kunden durch sich verändernde Märkte und Ökosysteme und unterstützt sie dabei, in diesem Wandel die führende und gestaltende Rolle einzunehmen. Unsere Mitarbeiter verfügen über tiefgreifende Industrieerfahrung und kennen die Trends von morgen und ihre Auswirkungen auf einzelne Branchen. Arthur D. Little unterhält Büros in den wichtigsten Wirtschaftszentren der Welt. Wir sind stolz darauf, für viele der Fortune 1000 Unternehmen weltweit sowie andere Marktführer und Organisationen des öffentlichen Sektors tätig zu sein.

Für weitere Informationen besuchen Sie bitte **www.adl.com**

www.adl.com/DigitalSignatures_german