



**ENTRUST**

# itAgile bildet Vertrauen in einer papierlosen Welt mit Entrust

itAgile

PRIME Cert TSP

## **GESCHÄFTSMÖGLICHKEIT**

Als Anbieter von Lösungen für digitale Dokumente und Signaturen wollte itAgile seine Kunden dabei unterstützen, Trusted Service Provider (TSP) zu werden, indem ein Produkt geschaffen wird, das es ihnen ermöglicht, die Anforderungen der TSP-Zertifizierung gemäß der eIDAS-Verordnung (electronic Identification, Authentication and Trust Services) zu erfüllen und schneller auf den Markt zu kommen.

eIDAS wurde entwickelt, um einen Rahmen für elektronische Transaktionen zu schaffen, der rechtsverbindliche grenzüberschreitende Geschäfte in der gesamten Europäischen Union (EU) ermöglicht. Sie schafft Standards, für die elektronische Signaturen die gleiche rechtliche Stellung erhalten wie ihre „wet-ink“-Äquivalente, und sieht die Regulierung von Trusted Service Providern (TSPs) durch Aufsichtsbehörden innerhalb ihrer jeweiligen Mitgliedstaaten vor.

« **Wir sind vertraut mit nShield Solo; es ist ein grundlegender Bestandteil des Systems. Das System ist erfolgreich, und die Zusammenarbeit mit dem Entrust-Team und seinem nShield HSM war eine positive Erfahrung, die es uns ermöglicht hat, eine kurze Markteinführungszeit zu erreichen und unsere Kosten zu amortisieren.** »

- Gianni Sandrucci, CEO bei itAgile

Im EU-Raum tätige Unternehmen profitieren von Vertrauensdiensten, die der Verordnung entsprechen: Alle unterzeichneten Dokumente und Vereinbarungen sind in der gesamten EU gültig. Vor allem Banken machen sich die eIDAS-Verordnung zunutze, um die Identität ihrer Kunden und die Gültigkeit ihrer Verträge zu gewährleisten. Im Zuge der Ausweitung ihrer digitalen Dienste auf ihre Bürger verlangen Regierungen auch die Verwendung von eIDAS-konformen Diensten und Signaturen.

### **TECHNISCHE PROBLEMSTELLUNG**

Die Lösung von itAgile würde eine Certificate Authority (CA) umfassen, eine Kernkomponente einer Public-Key-Infrastruktur (PKI), die für den Aufbau einer hierarchischen Vertrauenskette verantwortlich ist. PKIs umfassen die erforderliche Hardware, Software, Richtlinien, Verfahren und Prozesse, um zu gewährleisten, dass ein Unterzeichner derjenige ist, für den er sich ausgibt.

CAs stellen die digitalen Berechtigungsnachweise aus, die zur Zertifizierung der Identität von Benutzern und zur Gewährleistung der Sicherheit einer PKI und der von ihnen unterstützten Dienste verwendet werden. CAs können daher das Ziel von ausgeklügelten gezielten Angriffen sein. Um das Risiko von Angriffen auf CAs zu verringern, werden physische und logische Kontrollen sowie Härtingsmechanismen, wie zum Beispiel Hardware-Sicherheitsmodule (HSMs), eingesetzt, um die Integrität einer PKI zu gewährleisten.

Gianni Sandrucci, Chief Executive Officer von itAgile, stellt fest: „Es ist eine ziemliche Herausforderung, eine Zertifizierungsstelle aufzubauen, die die Anforderungen des eIDAS TSP erfüllt. Sie müssen 360 Anforderungen erfüllen, um die TSP-Zertifizierung zu erhalten. Zu den Anforderungen gehört die Verwendung von

HSMs, die nach Common Criteria EAL4, dem Sicherheitsstandard für kryptographische Lösungen, zertifiziert sind. Geeignete HSMs sind auf dem Markt nicht leicht zu finden. Außerdem ist die Kryptographie selbst keine klare und einfache Angelegenheit.

### **LÖSUNG**

Als Experten für digitale Signaturen wählte itAgile die nShield Solo HSMs von Entrust aus, die nach Common Criteria EAL4+ zertifiziert und als qualifizierte Signaturerstellungsgeräte (QSCDs) anerkannt sind. TSPs sind verpflichtet, QSCDs mit starker Kryptographie zu verwenden, um die Sicherheit ihrer Signaturen zu schützen.

Laut Sandrucci sind „HSMs der Kern des Prozesses. Wir brauchen ein HSM, um die Wurzel des Vertrauens zu schaffen, zwei für PKI-Operationen, wie z. B. die Ausstellung und Validierung von digitalen Zertifikaten und Signaturen, und eines für die Notfallwiederherstellung. Diese Architektur bietet ein doppeltes Maß an Sicherheit, da sie den Root-Schlüssel und die CA voneinander trennt. Ein HSM schafft die Vertrauensbasis, das andere erstellt die Zertifikate.

Darüber hinaus muss unser Service sehr zuverlässig sein, was mit der Zuverlässigkeit des Entrust nShield® HSM einhergeht. Nicht zuletzt aus diesem Grund haben wir uns für Entrust entschieden. Ihre HSMs sind verlässlich und halten viele Jahre an“.

### **ERGEBNISSE**

Der PrimeCert TSP von itAgile bietet Kunden eine schlüsselfertige Lösung, die es ihnen erlaubt, ein qualifizierter TSP zu werden. Der PrimeCert-Kunde ist immer noch verpflichtet, die eIDAS-Zertifizierung zu erlangen, aber alle Teile für die Zertifizierung sind vorhanden. Und eines der wesentlichen Stücke ist das Entrust nShield Solo HSM, das nicht nur nach Common Criteria EAL4+, sondern auch nach FIPS 140-2 Level 3 zertifiziert ist.

« **Darüber hinaus muss unser Service sehr zuverlässig sein, was mit der Zuverlässigkeit des Entrust HSM einhergeht. Nicht zuletzt aus diesem Grund haben wir uns für Entrust entschieden. Ihre HSMs sind verlässlich und halten viele Jahre an.** »

- Gianni Sandrucci, CEO bei itAgile

Gianni Sandrucci bemerkt: „Die EU ist stark reguliert. Wenn einer unserer Kunden papierlos arbeiten möchte, muss er zunächst die EU davon überzeugen, dass sein System mit der eIDAS-Verordnung konform ist. Mit den Entrust nShield Solo HSMs erfüllt unser Produkt alle aktuellen Regeln sowie das, was wir für die nächste Generation von Regeln erwarten“.

„Wir sind vertraut mit nShield Solo; es ist ein grundlegender Bestandteil des Systems. Das System ist erfolgreich, und die Zusammenarbeit mit dem Entrust-Team und seinem nShield HSM war eine positive Erfahrung, die es uns ermöglicht hat, eine kurze Markteinführungszeit zu erreichen und unsere Kosten zu amortisieren.“

## ÜBER ITAGILE

itAgile ist auf agile digitale Dokumenten- und Signaturlösungen in Italien und der restlichen Europäischen Union (EU) spezialisiert. Das 2008 gegründete Unternehmen bietet seinen Kunden und Partnern

- Best-of-Breed-Produkte
- Umfassende Kenntnisse der Gesetzgebung und Normen
- Technischen Support
- Anwendungsentwicklung für die effiziente Integration von Produkten in Kundenprozesse

Das nach ISO 27001 und ISO 9001 zertifizierte Unternehmen itAgile hat ein flexibles, unkompliziertes Organisationsmodell, mit Fokus auf Kundenservice und basierend auf dem Einsatz von Cloud-Technologien und innovativen Hilfsmitteln für Zusammenarbeit.

### Geschäftliche Anforderungen

- Erstellen einer schlüsselfertigen Lösung, damit Kunden mit digitalen Signaturen die eIDAS TSP-Zertifizierung erhalten und schneller auf den Markt kommen können.

### Technische Anforderungen

- Erstellen eines replizierbaren Prozesses, der zahlreiche, strenge technische Anforderungen erfüllt, die zum Erreichen des eIDAS-qualifizierten TSP-Status erforderlich sind. Dazu gehören CAs, die nach Common Criteria EAL4+ zertifizierten HSMs geregelt sind.

### Lösung

- Entrust nShield Solo HSMs

### Resultat

- Schnellere Markteinführung für itAgile Kunden, die eine TSP-Strategie verfolgen

## ÜBER ENTRUST

Entrust ermöglicht vertrauenswürdige Identitäten und Zahlungen sowie verlässlichen Datenschutz und hält damit die Welt sicher in Bewegung. Ein nahtloses und sicheres Umfeld ist heute mehr denn je unerlässlich, sei es bei Grenzüberritten, beim Einkaufen, beim Zugriff auf E-Government-Dienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet für genau diese Interaktionen eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen. Mit 2.500 Mitarbeitern und einem weltweiten Partnernetzwerk ist Entrust für Kunden in über 150 Ländern tätig, die sich bei ihren sensibelsten Operationen auf uns verlassen.