DATASHEET

GlobalSigns Digital Signing Service vs. HSM-implementaties

Implementaties van digitale handtekeningen voor organisaties met behulp van software voor het automatisch genereren van documenten, workflow- of beheersoftware

Tot voor kort kozen organisaties die digitale handtekeningen wilden integreren in documentworkflows vaak voor het gebruik van een HSM (op locatie of in de cloud). Het configureren van de integratie tussen de HSM, de documentsoftware en de verschillende cryptografische componenten die nodig zijn om handtekeningen te implementeren is niet altijd even eenvoudig (bv. handtekeningcertificaten, sleutelbeheer, tijdstempelserver, OCSP- of CRL-service). Hiervoor zijn interne ontwikkelingsresources met geavanceerde cryptografische kennis vereist.

Gelukkig heeft GlobalSign een nieuwe cloud-based Digital Signing Service (DSS) ontwikkeld om dit soort integraties te vereenvoudigen en vertrouwde, conforme digitale handtekeningen toegankelijker te maken voor organisaties van elke grootte. In tegenstelling tot HSM-implementaties, waar u de cryptografische componenten afzonderlijk beschikbaar moet maken en uw toepassing moet instellen om afzonderlijke oproepen te doen naar elke service, omvat DSS al deze componenten in één REST API, met minimale ontwikkeling en overheadkosten.

Organisaties die momenteel een HSM-implementatie voor digitale handtekeningen gebruiken, of dat van plan zijn, doen er goed aan om de ondertekeningsservice te migreren om de volgende redenen:

- Investeringen in of het onderhoud van een HSM overbodig maken.
- De integratie en ontwikkeling vereenvoudigen om digitale handtekeningen te implementeren in documentsoftware, een native verbinding met HSM en andere cryptografische componenten overbodig te maken (d.w.z. interne ontwikkelingsresources besparen en geen nood aan interne PKI-expertise).
- Meer flexibiliteit krijgen bij ondertekeningsidentiteiten (d.w.z. HSM-oplossingen kunnen alleen ondertekenen met identiteiten op organisatieniveau; DSS ondersteunt individuele identiteiten).
- De schaal van de implementatie gemakkelijker aanpassen indien nodig (d.w.z. voor HSM-implementaties zijn eventueel bijkomende partities of configuratie nodig).
- De nood aan intern beheer van de private keys wegnemen (dit gebeurt door DSS API).
- Standaard hoge beschikbaarheid garanderen, zonder redundante HSM-investering.

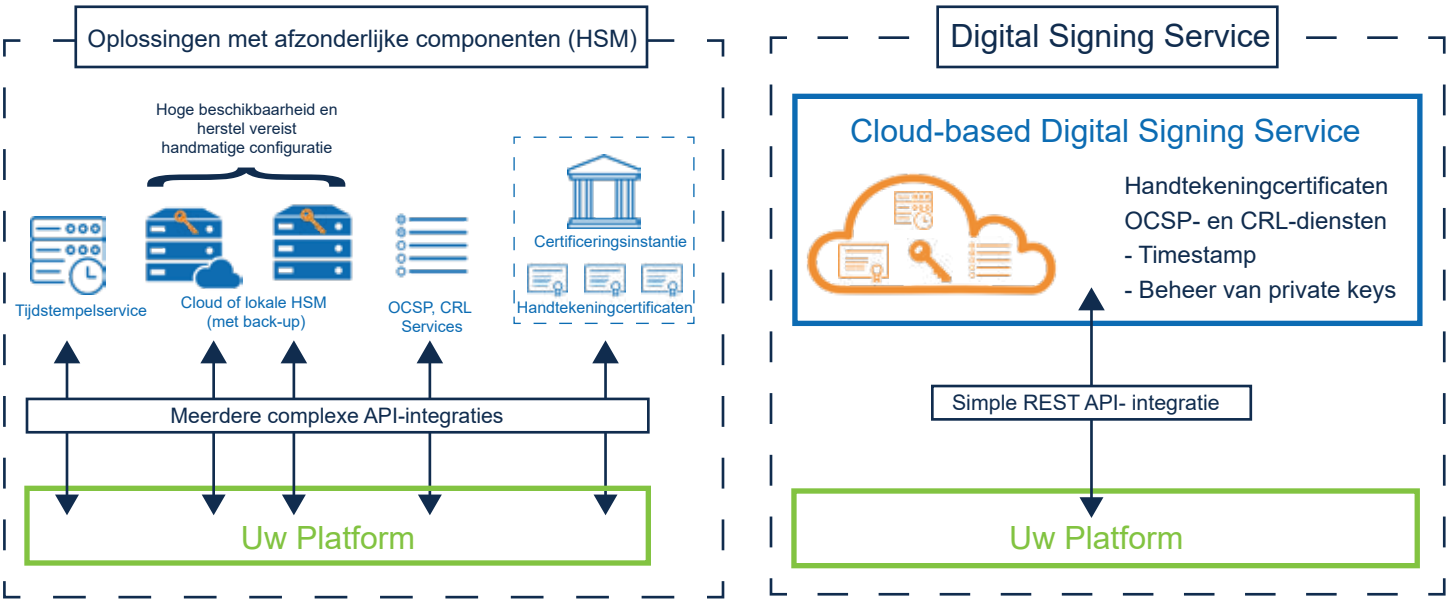
Kenmerken

- **Eenvoudige integratie met documentworkflow/software**
  Cryptografische componenten die nodig zijn voor handtekeningen worden beschikbaar gemaakt via een eenvoudige REST API, in tegenstelling tot meerdere calls voor elke component
- **Geen interne PKI-expertise vereist**
  Integratie met documentsoftware is veel eenvoudiger en beheer van private keys gebeurt door de service (d.w.z. GlobalSign)
- **Flexibiliteit van identiteiten**
  Individuele identiteiten en identiteiten op organisatieniveau worden ondersteund, in tegenstelling tot HSM-implementaties die doorgaans slechts organisatieniveau ondersteunen
- **Tijd en middelen besparen**
  Geen investering in en onderhoud van een HSM nodig, plus vereenvoudigde integratie bespaart kosten voor ontwikkeling en hardware

GlobalSign®
GMO INTERNET GROUP

HSM-implementaties vs. GlobalSigns Digital Signing Service

	HSM-implementatie	Digital Signing Service
Integratie met toepassingen voor het ondertekenen van documenten	Interne cryptografische expertise voor configuratie en beheer vereist	Via simple REST API
Identiteit van ondertekenaars	Alleen identiteiten op organisatie- of afdelingsniveau worden ondersteund (bv. boekhouding)	Ondersteuning van individuele identiteiten én afdelingsniveau (bv. Peter Jansen, boekhouding)
Schaalbaarheid	Mogelijk bijkomende HSM-partities en configuratie nodig	Geen bijkomende configuratie of integratie nodig
Documentworkflow-opties	Een ondertekeningsworkflow op maat ontwikkelen of integreren met Adobe LiveCycle, Ascertia DSS, Eldos Secure Black Box en iText Java/C	Naadloze integratie met een groeiende lijst van partners, zoals Ascertia en Odyssey
Beheer van private keys	Klant verantwoordelijk voor sleutelbeheer	Uitgevoerd door REST API (geen interne middelen vereist)
Cryptografische handtekeningcomponenten (bv. certificaten, OCSP, CRL, tijdstempels)	Apart beschikbaar, moeten apart worden aangeroepen door toepassing en interne ontwikkelingsresources voor configuratie	Gebundeld in één API, geen geavanceerde cryptografische kennis of ontwikkelingsresources nodig



Over GlobalSign

GlobalSign is de grootste aanbieder van betrouwbare identiteits- en beveiliging-soplossingen waarmee bedrijven, grote ondernemingen, cloudserviceproviders en IoT-vernieuwers wereldwijd hun online communicatie kunnen beveiligen, miljoenen geverifieerde digitale identiteiten beheren en authenticatie en encryptie automatiseren. Zijn grootschalige Public Key Infrastructure (PKI) en identiteitsoplossingen ondersteunen de miljarden services, apparaten, mensen en dingen die deel uitmaken van het internet der dingen.

US: +1 877 775 4562
UK: +44 1622 766766
EU: +32 16 89 19 00
verkoop@globalsign.com
www.globalsign.nl

GlobalSign
GMO INTERNET GROUP