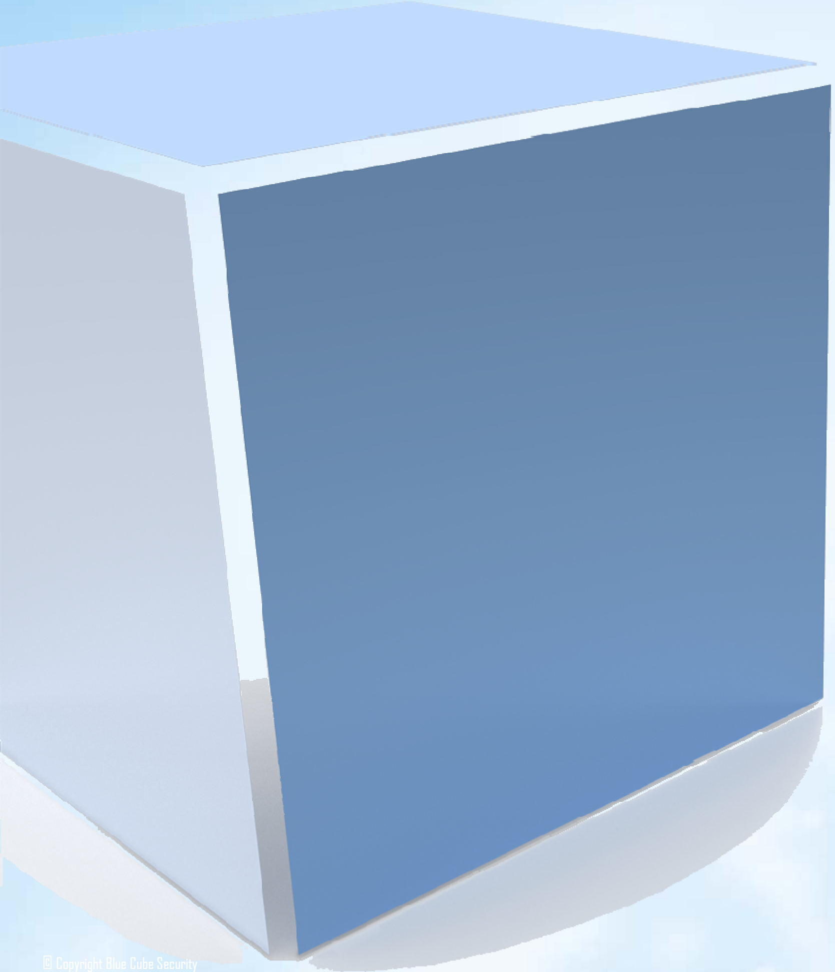


Rod Crook– Solutions Director, Ascertia

Nick Munro – Technology Services, Blue Cube Security

Real world deployment of remote signing technology.

Business Requirement

- 350,000 contracts a year
- Consumers, not previously known, probably not seen again
- High assurance (AATL) PDF signing
- Trust must be survivable past the end of the system life, and portable
- Driven by paperless desire, but simple UI needed
- User experience paramount for signing customers
- Offer dealership or home based remote signing ability

Technical Requirement

- Follow ISO 32000/19005 PDF, ETSI PAdES LTV/LTA standards
- Up to a 5 year agreement, FCA require 5 years validity beyond that
- HSM required for key generation and signing
- Integration with existing financial document workflow system
- Public cloud hosting with 24x7x365 availability
- Mobile device compatibility
- Short life certificates (single session use)
- Satisfies AATL registration requirements

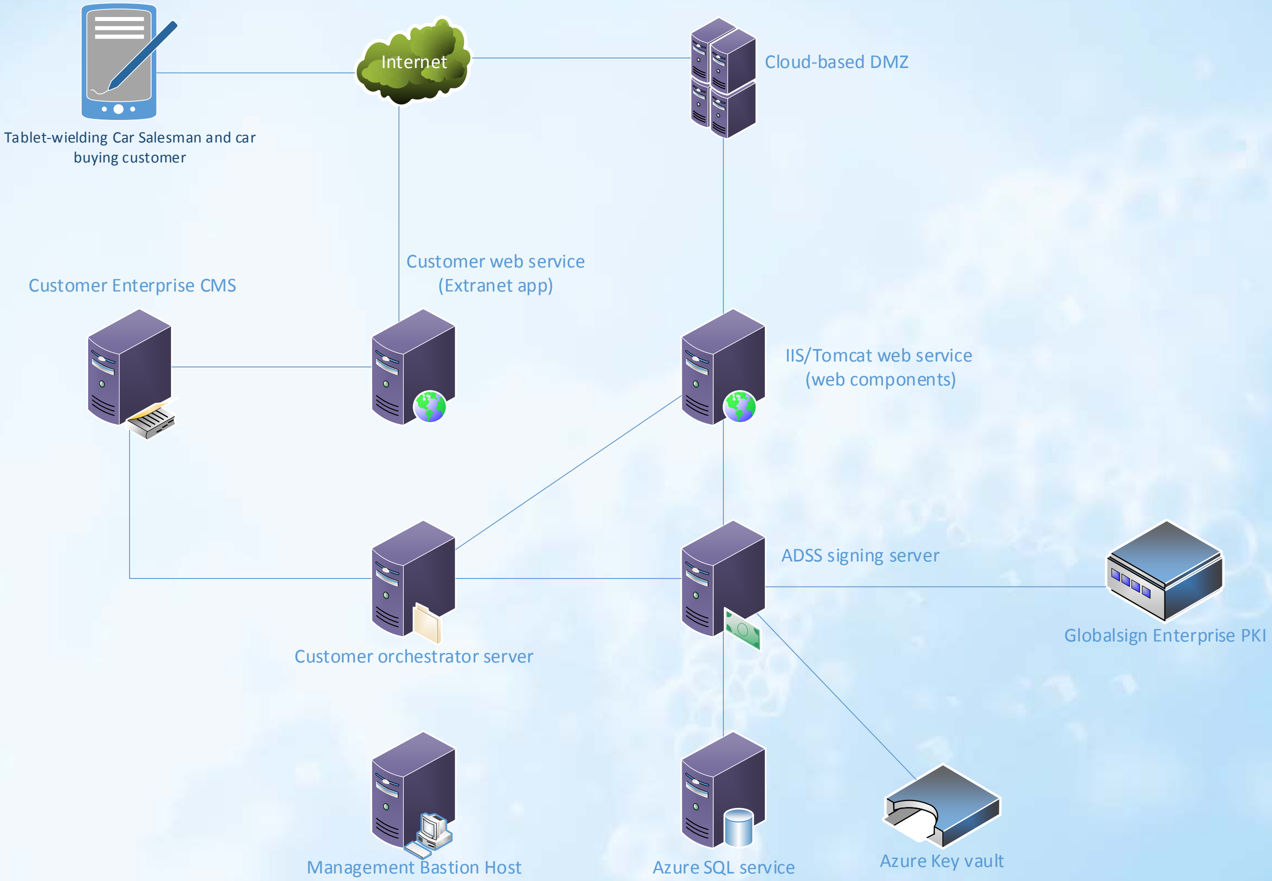
Architecture

- Customer application in corporate network, and orchestrator app in Azure.
- Enterprise service bus into Azure
- Front-end SigningHub web service in Azure
- Back-end ADSS Server in Azure
- Trusted link to HSMs at Trustis
  - Replaced by link to Azure Key Vault
- Link to GlobalSign Enterprise PKI for certificate and time stamps

Architecture

ascertia

Blue Cube
Intelligent Protection



Tablet-wielding Car Salesman and car buying customer

Internet

Cloud-based DMZ

Customer Enterprise CMS

Customer web service (Extranet app)

IIS/Tomcat web service (web components)

Customer orchestrator server

ADSS signing server

Globalsign Enterprise PKI

Management Bastion Host

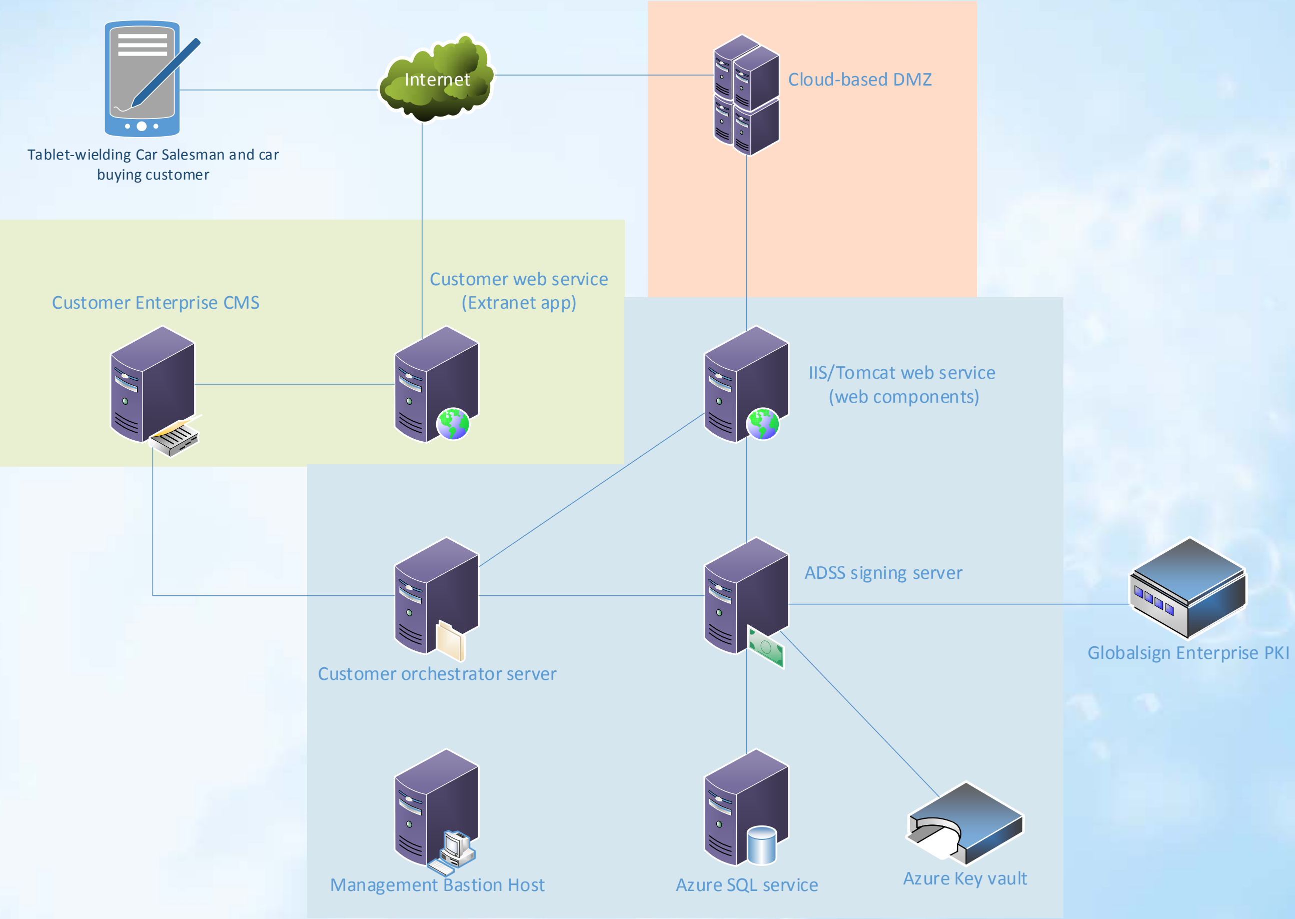
Azure SQL service

Azure Key vault

Architecture

ascertia

Blue Cube
Intelligent Protection



Tablet-wielding Car Salesman and car buying customer

Internet

Cloud-based DMZ

Customer Enterprise CMS

Customer web service (Extranet app)

IIS/Tomcat web service (web components)

ADSS signing server

Globalsign Enterprise PKI

Customer orchestrator server

Management Bastion Host

Azure SQL service

Azure Key vault

Issues

- HSM capacity is an issue- keys are short lived so need to be managed in limited space.
- HSM latency- over VPN
- Availability and responsiveness at CA, cloud service provider
- 5-way shared responsibility in support
- Registration requirements- leveraged KYC routine from finance world.
- Commercial key vault pricing not geared for short lived high volume key pairs
- Contractual relations- sub CA, registration terms, AATL program terms

Opportunities

- It works- this system survived contact with the public.
- Over 30,000 documents per month signed in March.
- Very large numbers of internal/external participants can use remote signing of documents to a high trust level, as viewers, signers and approvers.
- Repeatable- for other AATL CAs and QTSPs.
- Takes careful planning in expectation setting, technical solution, and service planning.
- Similar solutions can be used in financial services, government and legal sectors subject to registration and processing requirements.

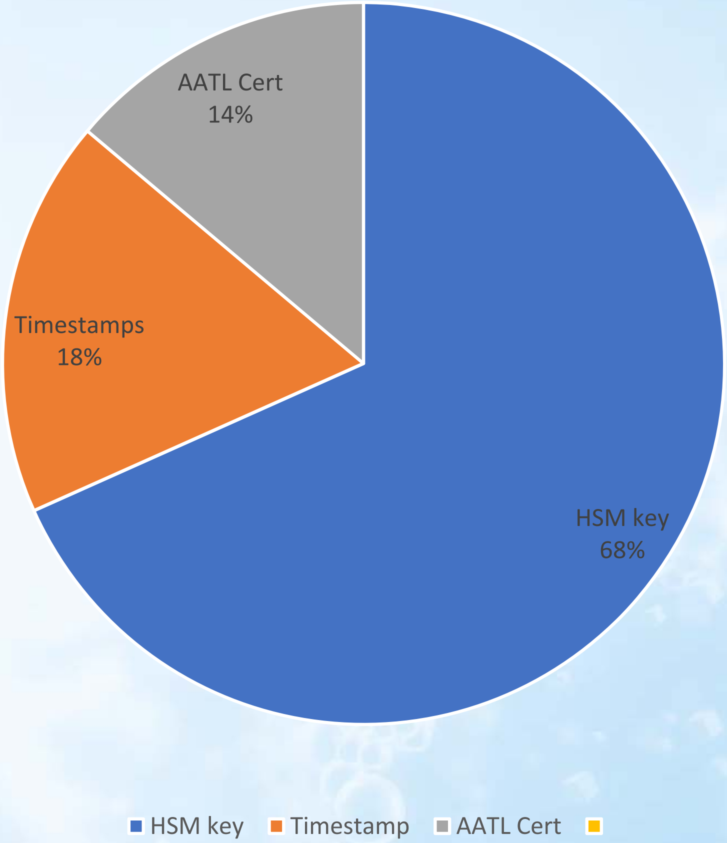
ascertia

Blue Cube
Intelligent Protection

Fin.

- Additional slides that probably won’t be shown unless someone asks.
- Do Not Scroll Farther Than This.

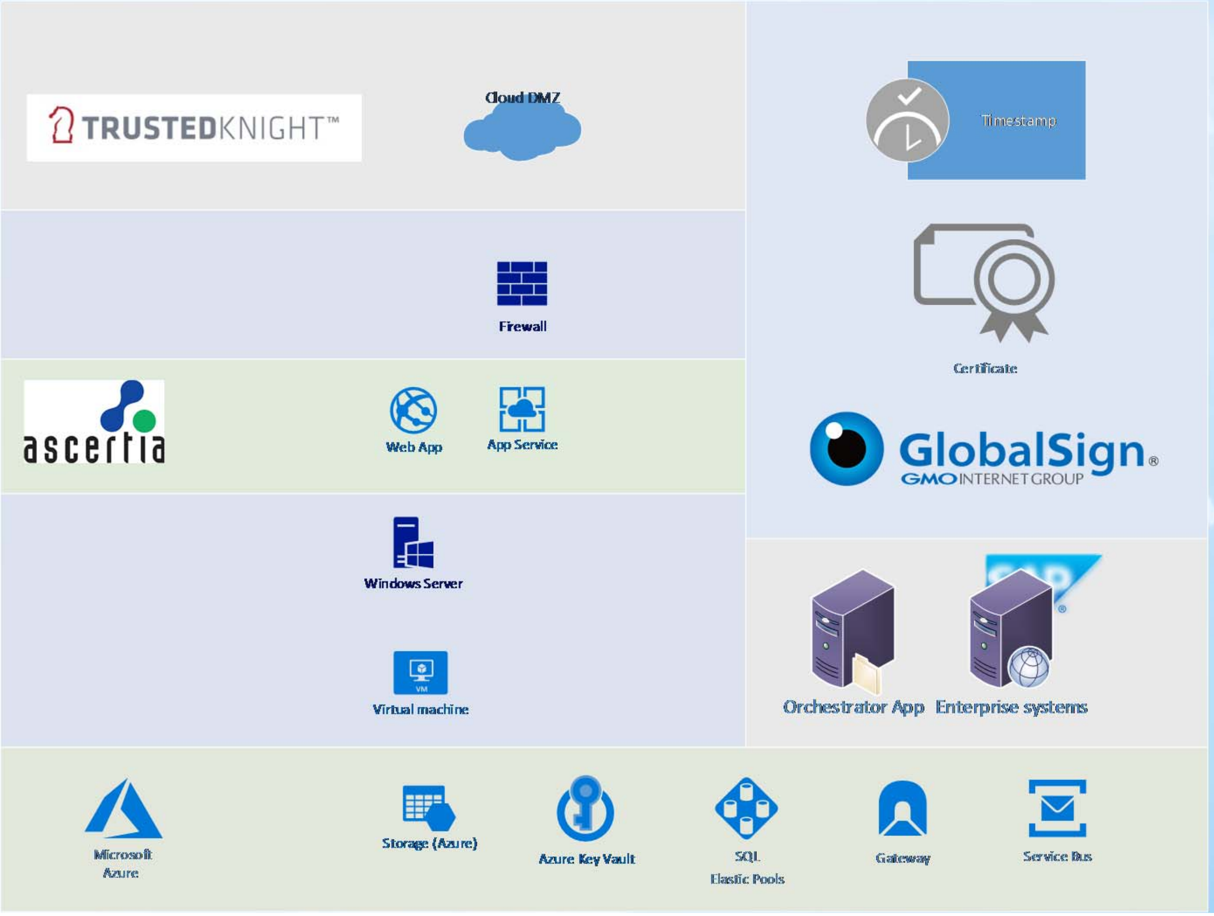
Incremental cost per document



Azure Key Vault Pricing

- How am I billed for HSM keys?
  - Each key that you generate or import in an Azure Key Vault HSM will be charged as a separate key. You will get charged for a key only if it was used at least once in the previous 30 days (based on the key's creation anniversary date). Note that if you store multiple (historical) versions of a given key, then each version is treated as a separate key for billing purposes.

Support Stack



TRUSTEDKNIGHT™

Cloud DMZ

Firewall

ascertia

Web App

App Service

Windows Server

Virtual machine

Timestamp

Certificate

GlobalSign®
GMO INTERNET GROUP

Orchestrator App

Enterprise systems

Microsoft Azure

Storage (Azure)

Azure Key Vault

SQL Elastic Pools

Gateway

Service Bus