Managed PKI

Solution Brief

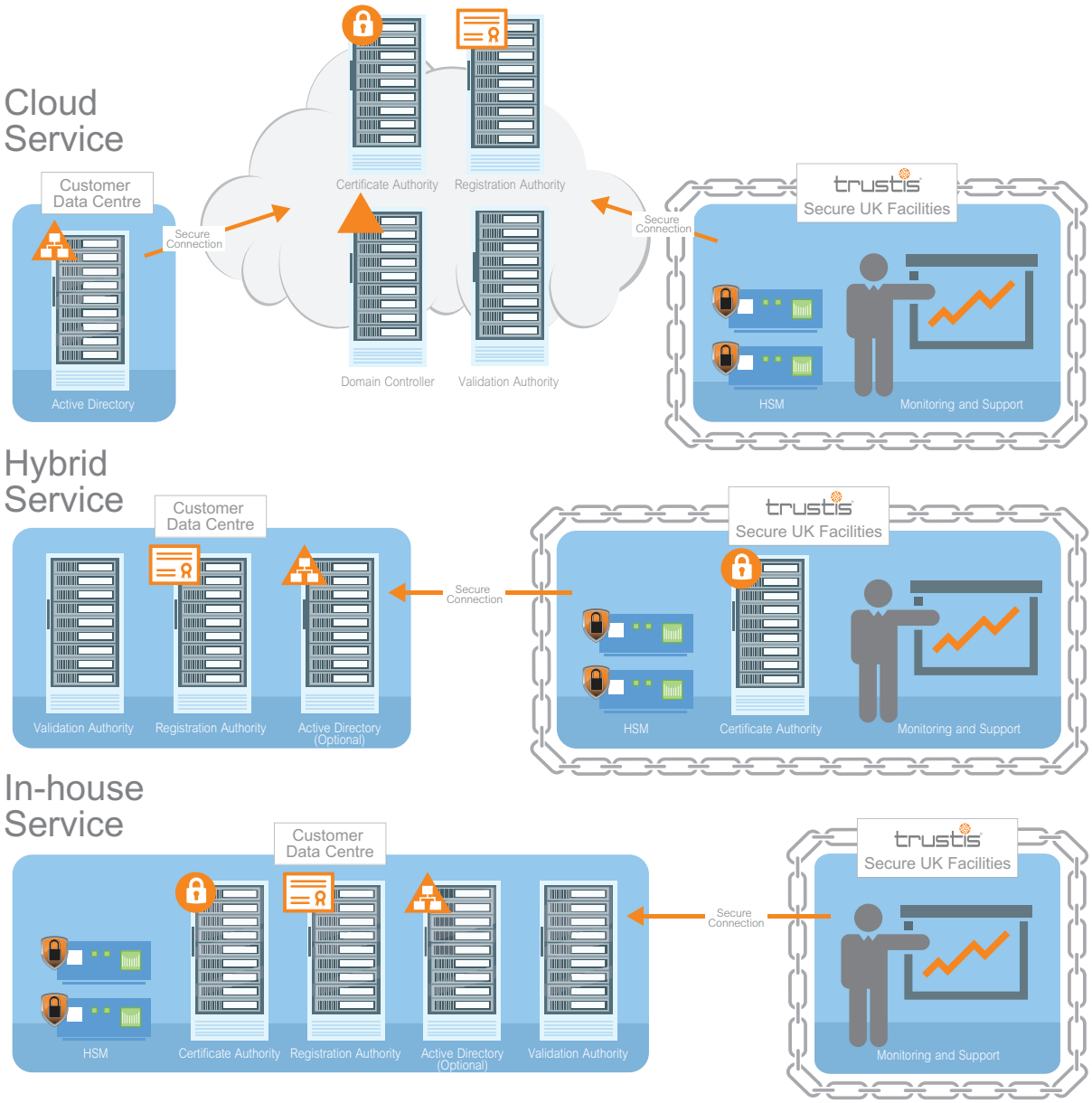
+44 (0)1635 231361
+44 (0)1635 231366
info@trustis.com
www.trustis.com

Trustis Managed PKI

End-to-end managed service for a secure, compliant PKI that's custom-built to satisfy your requirements.

Key Points

- Bespoke design and build using proven architectures and policy structures
- Streamlined management of the certificates that secure user, device and application identities
- Complete control over your Public Key Infrastructure (PKI), expertly managed
- Provided in a hosting model that suits you best
- Cost-effective, flexible and low risk



Maintaining a Compliant, Reliable PKI Service: The Challenge

Building and operating a PKI to tScheme or other rigorous assurance standards is a specialist undertaking. An array of expert skills is required throughout the process to ensure requirements are met, to achieve compliance and to deliver a reliable business service.

Organisations that operate PKIs realise, through experience, that the overheads of running a PKI in-house can be significant. In addition to maintaining the highly-controlled environment, there are essential management activities such as key ceremonies; policy and procedure documents including a Certificate Policy (CP) and Certificate Practice Statement (CPS) to develop and govern it; audit activities; server/HSM refreshes; software/security updates, etc. Equally, organisations that issue credentials to third parties or that digitally sign external documents have to recognise the level of liability associated with providing these credentials from their PKI.

Trustis Managed PKI: The Solution

Using our assured PKI Builder methodology, Trustis has built and operated over 100 standards-compliant PKIs for organisations including Governments, defence, telecommunications, utilities, financial, media and pharmaceutical companies. Our methodology covers all aspects of the technical build as well as the policy requirements and procedures to maintain high levels of assurance and any necessary accreditation.

In-house or cloud managed service

To give you optimum flexibility, Trustis offers several options for operating and managing your PKI:

- In-house service: The PKI is deployed by Trustis and remotely managed and supported.
- Cloud service: The entire PKI is hosted by Trustis, either in our highly secure, ISO27001 certified, tScheme-accredited facilities, or in your preferred cloud provider such as Microsoft Azure or Amazon Web Services. The customer interface is via a web portal and/or VPN.
- Hybrid service: Key components of the PKI – such as the Root Certificate Authority (RCA), possibly the sub-CAs and the Hardware Security Modules (HSMs) – are hosted by Trustis. The other components, such as Registration Authorities (RAs), are housed in the customer's data centre and remotely managed and supported.

All our PKIs are built to best practice, are standards-based, compliant with tScheme assurance rules and operate under English Law.

Customer dedicated solution

Offline Root CAs are implemented on hardware and operating systems provided at the Trustis Service Centre (TSC) secure facilities. The Root CA is operated within Trustis' Certificate Factory, which ensures that the build and operations are controlled and assured to tScheme. This provides the foundation for any subsequent specific requirement for tScheme approval of the Root CA, subordinate CAs or PKI services in your organisation's name.

Multiple Issuing CAs can be provisioned easily if different policies are required for different certificate types. Certificate management for certificate issuance, vetting, revocation and audit are provided via a secure web portal interface protected by two-factor authentication. Enrolment is provided by direct connection or secure VPN and exposing interfaces, such as SCEP, CMP or Active Directory for device certificate auto-enrolment, which is a common function these days.

As part of the solution, Trustis develops a bespoke Certificate Policy (CP) for each customer's service. The Root CA of the solution is generated under an audited Key Signing Ceremony where the customer is the custodian of the cryptographic key share, ensuring they retain authority.

The PKIs can issue and manage:

- Server Certificates: TLS / SSL, domain controller
- Device Certificates: desktop, laptop, embedded device, Wi-Fi
- Smart Card Credentials: logical and physical access
- Mobile Device Certificates: support for iOS, Android, BlackBerry and Windows
- User Certificates: authentication, signing, encryption

Benefits of Trustis Managed PKI

- Rapid and simplified deployment using proven templates and policy structures
- Reduces risk by maintaining security though tScheme-assured processes
- Provides best-practice PKI management processes for your business
- Bespoke registration and vetting design to fit your business processes
- Consistent and robust control over the lifecycle of certificates to mitigate risk
- Significant cost savings over in-house deployments
- Scaled to your requirements
- Supports multiple business units and role-based access
- Can be deployed on different CA technologies to suit customer requirements

Key Features and Technical Specifications

- Custom designed and built PKI
- High-assurance PKI service
- Customer-specific Certificate Policy
- Support for device/computer, Wi-Fi, mobile device, SSL/TLS and user certificates
- Infrastructure and cryptographic keys managed to tScheme assurance standards
- Services run from UK in ultra-secure, purpose-built facilities
- Only the customer has access to the HSM-stored Root CA private keys
- Highly-redundant infrastructure with intelligent monitoring and full disaster recovery
- PKI software/hardware evaluated against Common Criteria and FIPS140-2-Level 3
- Customer interface via web portal and/or VPN

Contact:

Robert Hann • Commercial contact

robert.hann@trustis.com

+44 (0)7818 552411

Building 273, Greenham Business Park,
Thatcham, Berkshire RG19 6HN