



# Entrust Data Protection Solutions Professional Services



**ENTRUST**

SECURING A WORLD IN MOTION

# Contents

- Overview .....3
- Deployment services ..... 4
- Packaged installation services ..... 4
- Migration services .....5
- Training services.....5
- Health checks ..... 6
- Consulting and development services..... 8
- Packaged solutions.....10
- PKI design and implementation services ..... 12
- HyTrust Professional Services ..... 12
- Example use cases by vertical.....14





We deploy the right solution for each unique environment.

## OVERVIEW

The Entrust Data Protection Solutions Professional Services team offers unmatched expertise in the optimal deployment of Entrust nShield® solutions, and both architecting and implementing crypto solutions for the world's most security-conscious organizations.

Based on decades of experience, our consultants work closely with both our clients and partners to design and deploy the right solution for each unique environment, leaving the relevant team with the knowledge to maintain it for years to come. This catalog provides an overview of our offerings, which include product deployment and training services, health checks, consulting and development, fully packaged cryptographic solutions, PKI design and build, and more. Review the service summaries to learn more and please contact us when you are ready to get started.

# Deployment services

Entrust Deployment Services help demystify HSM installation, migrations, and management, accelerating time to value for nShield investments. Our deployment services ensure the quick and correct deployment of products, new solutions, and migrations from legacy nShield Platforms. We will help architect and configure the solution to meet the required use case(s) for each unique client environment and include training options that leave operational teams with the knowledge to maintain the solution for years to come. Our deployment services can be bundled as ready-made packaged offerings as part of any nShield solution. We can also create custom consulting packages for larger or complex deployments as required.

## Packaged installation services

### Hardware security module (HSM) rapid setup and deploy (PS-HSM-RD)

The HSM rapid setup and deploy service will help accelerate your deployment so you can start maximizing the potential of our products. Entrust Professional Services consultants will be with you throughout the deployment process, offering advice and transferring our knowledge and experience to your staff. We install up to four HSMs at a single site and provide informal training to your staff during the course of the installation.

### HSM install with training (PS-HSM-SI)

The Entrust HSM standard install engagement includes formal training of your personnel and deployment of nShield HSMs within your environment, deploying up to six HSMs at a single site. An Entrust consultant will work with your team to plan and document an efficient deployment strategy while delivering an nShield certified systems engineer (nCSE) training course covering nShield HSM cryptographic operations, features, encryption technology, and functionality.

### HSM enhanced install (PS-HSM-EI)

The Entrust HSM enhanced install engagement includes formal training of your personnel and deployment of nShield HSMs within your environment, deploying up to six HSMs at a single site. An Entrust consultant will work with your team to plan and document an efficient deployment strategy while delivering an nShield Certified Systems Engineer (nCSE) training course covering nShield HSM cryptographic operations, features, encryption technology, and functionality.

Then, after six months of HSM use in your environment, an Entrust consultant performs a healthcheck to verify proper operation, policies, and procedures.

### **Remote Administration rapid install (PS-HSM-RA-INST)**

Entrust nShield Remote Administration allows HSM owners to administer their HSMs from anywhere, saving time and money. The nShield Remote Administration rapid install delivers further time savings by helping organizations get up and running and realizing the benefits of this tool as quickly as possible.

## **Migration services**

### **Entrust nShield Key/Security World migration (PS-HSM-SWM)**

An Entrust Professional Services consultant will help you migrate your legacy Security Worlds to new, more secure versions to support the deployment of newer hardware. Your consultant will help you identify and plan for the migration, create the new security worlds, and migrate the keys to the new environment. This is often required for migrating from older, end-of-life equipment to new HSMs.

### **Cloud Concierge service (PS-CLS-CS)**

The Entrust Cloud Concierge service delivers a seamless transition from Entrust's traditional on-premises HSM environment to our nShield-as-a-service environment. Our experienced consultants will work with you to plan and execute the migration of existing keys, clients, and custom applications into our cloud environment.

### **Public key infrastructure (PKI) migration (PS-PKI-CONS)**

The PKI migration service will help you securely manage the complexities of the critical migration of your PKI from SHA-1 based certificates to SHA-2, or to migrate from older Windows 2008 Server CAs. An Entrust consultant will help you understand your options and support your migration as needed, from planning and documentation through testing and deployment.

## **Training services**

### **Entrust nShield Certified Systems Engineer training (PS-TRN-NCSE-O or PS-TRN-NCSE-C)**

The Entrust nShield Certified Systems Engineer course provides a comprehensive introduction to the whole Entrust nShield product family. With a mixture of theory and hands-on practical workshops, the nCSE course will provide delegates with the confidence and knowledge to deploy and set up a working security domain that can be fully aligned with your business security needs and requirements. This is available at your location (on-site), or in a regularly scheduled class at an Entrust location.

### **Entrust nShield Certified Solution Developer training (PS-TRN-NCSD-O or PS-TRN-NCSD-C)**

Entrust Certified Solution Developer training enables your team to quickly learn the skills needed to build, test, and deploy HSM applications using nShield HSMs. Certification helps ensure your developers are ready to leverage the complete capabilities of Entrust nShield HSMs, allowing your team to deliver projects faster and on budget. This is available at your location (onsite), or in a regularly scheduled class at an Entrust location.

### **PKI training (PS-TRN-PKI)**

Based on vital knowledge gained from years of PKI deployment and management, the Entrust Professional Services team will train your staff on the ins and outs of PKIs, equipping them to rapidly deploy and smoothly operate your system throughout its lifecycle. Designed for any team members involved in PKI operations, the training helps instill the skills your team needs to build your system and keep it running as efficiently as possible. This training is not designed to replace product-specific PKI training, but provides a more general overview of PKI topics, requirements, usage, and operations.

## Health checks

Entrust Data Protection Solutions health checks are designed to assess existing cryptographic solutions and infrastructure, from an architectural, configuration, policy, and governance perspective, aligned to the required business use cases and recommended best practices. On completion of the analysis, our consultants will provide both a written report and formal presentation to detail findings and recommendations.

### **HSM Health Check (PS-HSM-HC)**

The Entrust HSM Health Check verifies the health of your Entrust HSM deployment and leaves your team with the knowledge to keep systems maintained. As part of an onsite engagement, an Entrust consultant will review your deployment and provide written recommendations for system maintenance and suggested operational procedures. When complete, you'll have more confidence that your configurations are optimal, and that your HSM operational environment is the best it can be.

### **PKI Governance Health Check (PS-PKIHC-GOV)**

A proper PKI implementation goes beyond technology. It needs to demonstrate essential compliance standards for audits. In addition, your PKI should be built to support both current and future business requirements. Our experts can review your PKI policy documentation (CP, CPS, RPS, PDS) and review the roles, processes, and policies that have been established for your organization. Our experts will compare those policies with best practices, standards, and your business use cases and applications. Then, we will deliver actionable recommendations to provide you with clearly defined and formal documentation that's designed to close procedural gaps.

### **PKI System Health Check (PS-PKIHC-SYS)**

It's not uncommon for an organization to be operating a PKI that was originally deployed 10 or 20 years ago. This timeline typically surpasses resource tenure and creates a knowledge gap. Over that time, an organization is likely to have increased its digital sophistication and its number of use cases.

It's important that the technology and software that comprise your trust environment are up to date and adapt to changes in your business. For example, modern digital ecosystems typically require a PKI that can grow and add capacity - or one that can seamlessly interact with remote apps and modern systems. We can help guide your teams by assessing the status of your existing PKI implementation - including the equipment and algorithms in use - to help ensure it meets both current and future business requirements.

### **eIDAS Compliance Readiness Assessment (PS-CONS-EIDAS)**

Entrust recognizes the importance of eIDAS certification for remote signing solutions and offers a compliance Readiness Assessment to assess the current state and technical solution steps required to meet new eIDAS compliance requirements. The service consists of a series of assessment workshops and a recommendations document reviewing the high level design and architecture, and advice on migrating existing signing keys, bearing in mind that there may be millions of keys stored in a database. The objective of the recommendations is to meet the requirements of EN 419 241-2, and maintain performance.



# Consulting and development services

Entrust Data Protection Solutions Professional Services is an experienced global team that solves customer problems through secure applied cryptographic solutions. nShield HSMs are always “part of a solution” and never deployed on their own. We’ve developed many solutions that optimize our technology to meet customers’ use cases and wider objectives as well as supporting dozens of technology integrations. We have extensive development capability building specific solutions for unique client challenges.

Solutions Entrust consultants have developed include those to address emerging technologies such as blockchain/wallets, new or proprietary encryption algorithms, or custom key derivation. Many solutions require secure processes for execution inside the HSM, where our CodeSafe technology provides a more secure execution environment for data protection, such as secure payment, root of trust, and IoT solutions. In addition, Professional Services has developed many custom key management processes/interfaces, and other customer-specific encryption and data protection solutions.

## **Custom HSM development (PS-DEV-CUSTOM)**

One of the strengths of the Entrust nShield HSM is the ability to run applications in CodeSafe, nShield’s secure execution environment. This allows customers to deploy unique, secure solutions to support a wide range of use cases. Examples of custom HSM development include the execution of proprietary or niche encryption algorithms, packaging of secure payloads, and emulation of other services within the HSM. The possibilities are endless! See some of our example use cases later in this catalog for more details.

## **Custom HSM services (PS-HSM-CUSTOM)**

Entrust Professional Services can help you plan and execute extensive HSM rollouts, migrations, or other large, HSM-related projects. Our global footprint and unsurpassed knowledge of nShield HSMs can help you quickly gain value from your nShield investment.

### **Custom code support (PS-CCSS-DEV)**

Development of a custom HSM solution doesn't mean you're on your own! Our custom code support allows you to obtain support for your custom application the same way you enjoy support for the rest of Entrust's products. This provides you with one point of contact for all Entrust products and custom solutions. The service also entitles you to updates for the code, and any bug fixes required. You've invested in a great, secure application – and we can support it!

### **Expert developer support (PS-EDS-DEV)**

Many sophisticated organizations utilize the nShield platform to develop their own solutions, but occasionally need a little expert developer assistance. Our expert developer support allows you to purchase time to work with our developers to help your team as they build their own solutions. Leverage the years of nShield platform development experience as your team builds your own unique solution.

### **Custom consulting (PS-CONS-CUST)**

Entrust Professional Services consultants have decades of experience in the design, development, and execution of sophisticated applied cryptographic solutions. Our experienced consultants can work with you to help design and build solutions to ensure security is built in from the start.

### **BYOK deployment service package for cloud service (PS-HSM-BYOK)**

Cloud users new to HSM technology often find that expert assistance can make for a smooth and secure deployment. The BYOK deployment service package utilizes an Entrust nShield Edge HSM (sold separately) and Professional Services to quickly get you cloud-ready and in control of your sensitive data and keys in the cloud. An Entrust Professional Services consultant will come on-site to explain the technology behind BYOK, and walk you through the processes of generating your own keys and securely transferring them to your cloud service.

# Packaged solutions

Entrust Professional Services has developed a number of packaged solutions that address specific and repeatable use cases that leverage the power of our Entrust nShield technology.

## **Code Signing Gateway (PS-DEV-CSGW)**

The Code Signing Gateway service provides a range of flexible and centralized workflow automation functions that helps organizations successfully meet secure code signing requirements. The Code Signing Gateway is a customer-hosted server that runs an Entrust code signing application and is complemented by on-site installation and training delivered by Entrust Professional Services.

## **Double Key Encryption Integration Pack (PS-DEV-MSDKE)**

Double Key Encryption extends control and security of sensitive data in hybrid and cloud environments for Microsoft Azure Information Protection services. It is designed to help enterprises protect their most sensitive content in Microsoft 365, by applying two layers of security for content in Azure cloud, encrypting so even Microsoft does not have the ability to access the content. The customer owns and fully controls the key and the software that generates it with no Microsoft footprint. The solution integrates with certified Entrust nShield HSMs to provide a root of trust for the protection of the customer keys. Replacing Microsoft Hold Your Own Key (HYOK), Double Key Encryption does not require enterprise customers to operate their own Active Directory and Rights Management servers. Instead, customers are empowered to provide their own cryptographic keys in real time.

## **Entrust Tokenization Solution (PS-DEV-TOKEN)**

The Entrust Tokenization Solution protects sensitive data with format-preserving encryption and data masking. It can tokenize and mask sensitive data while maintaining the data format, utilizing a RESTful API that enables the integration of multiple programming language environments and reduces development effort and lead times. The solution provides strong key protection using FIPS 140-2 and Common Criteria certified Entrust nShield HSMs with a highly scalable micro services architecture that supports a variety of character sets. The solution provides data protection of structured data for compliance of personal data privacy, and for financial data protection.



### **Certificate delivery system (PS-DEV-CUSTOM)**

Entrust can help you securely deliver keys and digital identities to your smart products during manufacturing and provisioning. Our certificate delivery system works with your PKI and nShield HSMs to securely request and deliver digital certificates in unsecured manufacturing environments. We will work with your team to integrate this solution into your planned or existing manufacturing process.

### **SecurePIN (PS-DEV-CUSTOM)**

Entrust SecurePIN enables end-to-end encryption from your payment client to your tamper-resistant nShield HSM. The strong key management and cryptographic algorithm in SecurePIN is a proven secure end-to-end encryption that has been widely adopted by banks, online payment systems, and mobile payment systems.. Based on the strong cryptographic functionality provided by Entrust nShield HSMs, the SecurePIN solution offers a high standard of data protection.

Entrust's experienced Professional Services team will work with you to implement SecurePIN based on your organization's specific requirements.

# PKI design and implementation services

## **PKI Document & Deploy Service (PS-PKI-CONS)**

As part of our PKI Document & Deploy Service, an Entrust Professional Services consultant will work with you to assess your approach to certificates and PKIs and then document the requirements, proposed solution, and post-deployment tests, and agree with you on the deployment scope. The consultant will then deploy the PKI and develop and deliver all of the appropriate documentation, including a CP/CPS, operational procedures, and more. After deployment the consultant will work with your team to test the PKI to prove that the solution meets objectives and functions as designed.

# HyTrust Professional Services

## **DataControl HealthCheck Service (PS-HT-DCHC)**

The HyTrust DataControl HealthCheck Service is the best way to ensure that your newly implemented or long-running KeyControl servers are optimized for trouble-free operation. HyTrust DataControl HealthCheck Service provides a Professional Services team member to assess the status and general functioning of your DataControl implementation. Your KeyControl servers are analyzed and configured to follow established best practices, and product alerting is fully configured for trouble-free operation. You receive a customized report, which includes recommendations for all issues found. This service is delivered remotely.



### **DataControl QuickStart Service (PS-HT-DCQC-REM, PS-HT-DCQS-OS)**

HyTrust® DataControl™ QuickStart Service provides a HyTrust Professional Services team member for the deployment and configuration of HyTrust DataControl (HTDC) for up to 10 virtual machines (VMs). In addition, QuickStart provides best practices knowledge transfer on HTDC key features, function, and operation. This service is delivered either on-site or remotely over three contiguous days. We employ a delivery approach that is informed by years of experience installing, configuring, and deploying HyTrust DataControl. Our methodology is designed to accelerate the start of workload encryption and leave you with all the knowledge necessary to operate HyTrust DataControl.

### **KeyControl QuickStart Service (PS-HT-KCQC-REM)**

HyTrust® KeyControl™ Quickstart Service provides a HyTrust professional services team member for the deployment and configuration of HyTrust KeyControl (HTKC) for up to four KeyControl nodes in a single cluster. This service is delivered remotely in a single, contiguous session up to eight hours.

We employ a delivery approach that is informed by years of experience installing, configuring, and deploying HyTrust KeyControl. Our methodology is designed to accelerate the start of workload encryption and leave you with all the knowledge necessary to operate HTKC. This includes:

- System architecture review
- KeyControl cluster installation
- Integration of supported HSM, if applicable
- Review operational best practices such as backup, restore, high availability, and disaster recovery scenarios
- Review HyTrust support tools

### **DataControl Training (PS-HT-EDU-DCF-R, PS-HT-EDU-DCF-O)**

HyTrust DataControl Training is an instructor-led two-day course, delivered on-site or remotely, that prepares participants to install and configure the basic features and functionality of HyTrust DataControl. The course includes hands-on labs, giving attendees actual experience with the product. At the conclusion, students will be familiar with the essential features of DataControl required to effectively manage and configure the product in their environment.

# Example use cases by vertical

## Financial services

Entrust custom developments underpin financial services worldwide, from retail and corporate banking to payments and equities. Solutions include custom cryptography, access and authorization control, key management, and at-rest and in-motion encryption. Entrust nShield solutions underpin interbank payment schemes, for faster payments, check Imaging, and more.

## Secure manufacturing

High-tech manufacturers protect their smart products through secure key and certificate injection and firmware signing, all using HSMs to guard sensitive keys. Entrust has worked with a number of market leaders to secure digital rights and smart devices, protecting both company IP and consumers from counterfeits and unauthorized changes.

## Smart metering

The smart metering industry heavily depends on best-in-class high-performance cryptographic services. Entrust has worked closely with key players in the industry around the globe and built suites of APIs and CodeSafe applications to support national standards covering manufacturing and in-situ operation.

## Connected IoT devices

The use of digital identities to protect devices is a requirement in today's connected world. This allows manufacturers to securely identify, update, and control their products - and extend that security to their customers. Entrust has worked with a number of large manufacturers to securely create and deliver digital identities to the factory floor - even when that manufacturing environment may be located outside of a trusted location. Entrust Professional Services leverages nShield HSMs, PKI solutions, and custom integrations to deliver a solution tailored to your environment.

## Scale-out key management

Entrust Professional Services has delivered custom solutions to help customers super-scale key management to support millions of keys, all protected by Entrust nShield HSMs accessible from both Java and PKCS#11 interfaces.

## Cryptocurrency

Entrust has implemented cryptocurrency functions and algorithms using Entrust nShield HSMs and CodeSafe to protect digital wallets.

## Blockchain

Blockchain technologies are rapidly expanding, and a number of exciting applications of the technology are emerging. Entrust Professional Services leverages the cryptographic power of our nShield HSMs and develops use-case specific applications to enable our customers to quickly deploy their cutting-edge solutions.

## Crypto architecture

The use of cryptography in a wide variety of products is designed to help secure solutions as they are deployed in the market. This can include solutions to protect personal data and financial data, provision digital identities, integrate with payment solutions, and more. The plethora of solutions can often lead to a piecemeal architecture, introducing security and operational vulnerabilities. Entrust Professional Services has worked with a number of our customers to design and deliver a secure cryptographic architecture on which their solution can be deployed.



To find out more about  
Entrust nShield HSMs

**HSMinfo@entrust.com**

**entrust.com/HSM**

## ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at  
**entrust.com**



Contact us:  
**HSMinfo@entrust.com**