



Secure payments made simple

PT-X HSM Information Pack

The following document acts as an aid to guide you through the terminology used by us and your Bank during your setup process.

Hardware Security Module (HSM) - Introduction

HSM's provide an alternative to Smart Cards for those users looking to automate the process of authentication and/or submission. These submissions are supported by Bacstel-IP, however due to little or no human interaction, the security of the underlying system needs to be very high.

As with Smart Cards, a digital certificate is still required to sign files and authorize submissions; although they are no longer accessed from a Smart Card, but a certificate store instead. Using a HSM for Bacstel-IP submissions mean that more stringent security requirements need to be in place. One requirement is that all cryptographic keys and digital signatures must be protected in tamper-resistant hardware that is certified by Bacs.

HSM Components

Certificate Signing Request (CSR)

This is an instruction for the bank to generate a Certificate for your HSM. The CSR contains **Distinguished Name (DN)** data to identify your organization further. The bank may specify a particular format for the Distinguished Name (DN) field within the CSR or provide you with a set DN format to use.

These details will be entered when creating a certification request. This is the field Bacs and your bank will use to verify the submissions sent. Once you have provided us with your DN format we will create the request for you. The bank will send you instructions on how to send the request to them, usually the files will need to be written to disk and posted to the bank in a tamper-proof envelope.

Certificate

Using your CSR the Bank will create a Digital Certificate; this Certificate enables the signing and submission of files to the Bacstel-IP service.

Once you have sent us the certificate from the bank we will on-board this on to the HSM device and configure the settings for this to be used in your PT-X solution.