BANK OF SCOTLAND

Frequently Asked Questions – Hardware Security Module (HSM)

Frequently asked questions

Question: Do I need Smart Cards if I choose a Hardware Security Module (HSM) solution?

Answer: A software solution that utilises a Hardware Security Module does not require Bacstel-IP Smart Cards to perform its submission and report retrieval functions. However, the HSM is not able to give access to the Payment Services Website. In order to maintain your contacts and details on this website, Smart Card access is required. Therefore your Primary Security Contacts will require their own Bacstel-IP Smart Card.

Bacstel-IP Smart Cards will offer extra resilience to your solution - in the event of a failure with your HSM you will be able to sign and submit data files using Smart Cards (although you should check with your Solution Supplier that your software supports both HSM and Smart Card operation; if so, they will be able to provide you with the instructions on this mode of operation).

Depending on the manufacturer and model of HSM you are supplied with, the HSM may have its own Smart Card protection system to ensure only authorised operators can access the device. These smart cards are not the same as cards issued by the banks for access to Bacstel-IP.

Question: The HSM Subscriber Standard requires the production of a Procedures Manual. Is there a sample version of this document?

Answer: Because of the detail required performing some of the HSM functions and the differences in different manufacturers HSMs it is not possible to produce a sample procedures manual. Advice should be sought from your Solution Supplier or HSM Vendor.

Question: Who should fulfil the roles required in the HSM Standard?

Answer: Whilst there are no hard and fast rules about who should be assigned to the roles, the following candidates should provide the "best fit" for each. Note that all individuals who are holding one of the roles should be familiar with the industry HSM Subscriber Standard, adherence to which is mandatory, and your Organisation's Procedures, which must be developed in accordance with the HSM Standard.

Key Manager – has overall control of the Bacstel-IP Key Management functions. Will need to have in-depth knowledge of the HSM and all aspects of its operation. Will need to keep accurate records of all Certificate Requests and Key Pair operations. Will need to have sufficient authority to be able to control other role holders in performance of their duties. The ideal candidates are likely to come from an IT Security department and will probably be at managerial level within the Organisation.

Physical Security Manager – responsible for the HSM equipment and possibly the Server Hardware that communicates it, the Physical Security Manager should be somebody who has access control over the actual location where the HSM is installed. The ideal candidates may be Computer Room Managers or members of an IT Security department.

Application Administrator – should be somebody who has managerial control over the configuration of the Bacstel-IP software. The Application Administrator should be aware of which changes to the configuration are documented in the Procedures Manual. The ideal candidates are likely to come from the department providing IT Support to the Finance Department, or possibly a computer literate member of the Finance team who is managing the configuration of the software.

Auditor – Previous auditing experience would obviously be an advantage. An Auditor will need to be readily available to the installation environment, particularly when commissioning new Software, generating Key Pairs or requesting Certificates. The ideal candidates would probably come from an Audit or Compliance department.

Question: My bank application form asks me to name an HSM Contact for each certificate, but I can't find this in the HSM Standard. Why is it not documented, and whom should I name on the form?

Answer: The industry HSM Subscriber Standard defines the requirements to implement and maintain a secure environment for PKI Credentials using an HSM. The HSM Contact (Certificate Owner) operates within this environment and has a responsibility only for the data that passes through the system. Therefore the HSM Contact is not detailed within the HSM Subscriber Standard.

The name and contact details associated with the HSM Contact must be the person with responsibility for the HSM. The person could also be set up as a contact in their own right.

When selecting a HSM Contact, the customer should be in mind that the contact need not be involved in the day-to-day operation of the equipment, but will be the point of contact that the bank will turn to should there be any problems with the payment data being submitted.

The e-mail address should be a group or general e-mail address relating to your organisation.

The HSM Contact telephone and fax numbers will be the points of contact for the bank should there be any problems with the payment data being submitted.

Question: What happens if a required person is not available?

Answer: It is possible to assign more than one person to each of the roles, although an individual cannot perform more than one role at any moment in time. Therefore an organisation should consider the allocation of roles carefully to ensure that there is resilience and sufficient cover for each of the roles.

Question: Can my solution supplier do everything for me?

Answer: The HSM Subscriber Standard allows for a third party to perform Key Generation procedures and to load certificates onto a HSM prior to delivery. If the customer is delegating the responsibility to a third party (Bacstel-IP Software Provider) to generate the certificate request it is necessary for someone trusted from their organisation to be available to oversee the key generation process – the customer remains responsible for the certificate and the process. All HSM Certificate Requests need to be transported securely to your bank; each bank will have specific instructions on how this is achieved and who is required to undertake this action.

Members of the Organisation should perform all other procedures. It is important, therefore, to ensure that proper training is carried out for all personnel involved in the operation of an HSM environment. Your sponsoring Bank will require you to adhere to the HSM Standards as part of their Terms and Conditions for provision of their services and may reserve the right to inspect your processes and procedures.

Question: What do I need to audit?

Answer: The Audit Log should be completed each time a change is made that alters the state of the HSM or the application that uses it. For example, a new Certificate is requested, or time of a scheduled submission (to be secured using a certificate stored on the HSM) is altered.

Question: Is there a sample Audit Log?

Answer: An Excel document is supplied as an outline for an Audit Log. This should be reviewed to ensure it matches your environment.

Question: Where can I get help?

Answer: Voca can provide independent training courses to help understand the procedures, which can be tailored to specific brands of HSM. Your chosen Solution Supplier may also be able to provide assistance.

Question: How can I implement "dual control" for an operation that requires only one person to perform?

Answer: Where the HSM Subscriber Standard describes that an operation requires "dual control" but the physical process only requires one person (e.g. a command line instruction entered at a command console) it is sufficient for a second authorised person to monitor the process and sign the Audit Log to show that the operation was carried out in line with the documented procedures.

Question: What are the risks?

Answer: Part of the Terms and Conditions of use HSMs laid down by the Member Banks require the HSM Subscriber Standard to be adhered to. Non-compliance to the Terms and Conditions could result in the sponsor revoking certificates due to the security risks that ensue. Members may reserve the right to inspect policies and procedures as part of their Terms and Conditions for issuing certificates. If procedures are not followed there is a risk of fraudulent submissions being made from your software. Your organisation will be liable for any losses resulting from non-adherence.

Question: What should I do if procedures are not followed?

Answer: If a breach of procedure is discovered, you should notify your sponsor of the nature of the breach at the earliest opportunity. You should also train staff to ensure they understand the need to follow the established procedures. In such circumstances it is likely that new certificates will need to be issued by your sponsoring member and associated costs incurred.

Question: Can I "clone" my HSM?

Answer: Some Solution Suppliers advocate the cloning of an HSM to provide a duplicate unit to be used in the event of equipment failure. Before accepting this implementation you should check with your sponsor's documentation to ensure that cloning of HSM keys and certificates is allowed (not all sponsors will allow device cloning) Where cloning does occur please be aware that:

- A breach of procedure or any other key compromise will result in both devices being inoperable.
- A problem with a certificate (e.g. expired or corrupted) would be replicated on both units
- Resolution of certificate problems will need to be replicated on all cloned HSMs

It is recommended that a customer should implement more than one certificate and more than one HSM, ensuring that the expiry date of the certificates is different for each. Independent HSMs (a different certificate on each HSM) may provide the required resilience with lower maintenance.

Question: Can I "back-up" the keys on my HSM?

Answer: You should check with your sponsor's documentation to ensure that backup (or key replication) is permitted by your sponsor before implementing such a procedure.

Question: Can I choose my own HSM or use one already within my operation?

Answer: Customers are encouraged to purchase their HSM units from the supplier of their Bacstel-IP software. This will mitigate the risks if problems with the HSM occur, when otherwise the customer may be passed between Software Supplier and HSM manufacturer. If you still wish to purchase the HSM independently, the following criteria should be met:

Your existing infrastructure should meet or exceed the operational guidelines defined within the HSM Subscriber Standard for Bacstel-IP.

The HSM you choose or are using has been tested and approved by Bacs for use in conjunction with the Bacstel-IP software package you are implementing (bear in mind that some suppliers will only be working with a limited number of HSMs).

Your software supplier is willing to implement their solution with an HSM they have not provided (you will need to take care regarding the support of the package should there be any doubt around the HSM operation).

Question: What Information is required in a Certificate Request?

Answer: The certificate generation process for your HSM will need information from you to create a certificate with a 'distinguished name' that is unique to your organisation and the HSM. A separate request is needed for each certificate and it is recommended that the components that make up the distinguished name be as follows:

	Primary	Backup	DR Site
Common name	(Organisation) HSM Live	(Organisation) HSM Backup	(Organisation) HSM Backup
Organisation unit	(Primary Site Location)	(Backup Site Location)	(DR Site Location)
Organisation	(Organisation)	(Organisation)	(Organisation)
Country code	GB	GB	GB

You will need to check the exact requirements for Certificate Request formats with your bank and software supplier.

Please contact us if you would like this information in an alternative format such as Braille, large print or audio.