PSN Frequently Asked Questions (FAQ)

Introduction

We are keen to build a comprehensive source of help for our customers and suppliers, this is the first of our PSN FAQs and we will be adding to them regularly.

If you have a question about PSN we hope you will find the answer here, if however we haven't addressed your question send it to us as at psn@cabinet-office.gsi.gov.uk , putting PSN FAQ in the title, we will respond and publish the FAQ here to help others.

Where will I find more information about the PSN IA conditions?

Detailed information supporting all of the IA Conditions for PSN can be found at: http://www.cabinetoffice.gov.uk/sites/default/files/resources/PSN-IA-Conditions-Supporting-Guidance-v1-4.pdf

How can I procure a connection to the PSN?

If you are a customer, the simplest way is to use the PSN Connectivity (PSNC) framework http://gps.cabinetoffice.gov.uk.

What is the minimum/maximum contract period under the PSN Connectivity Framework?

There is a five year maximum period for all items, except Mobiles and Pagers which are three years. Contracts can be extended by up to two years to allow for transition. There is no minimum period.

How much does a connection cost?

PSN connections may be provided by any of the PSN-Compliant service providers. You may want to buy connections that are not PSN-compliant (e.g. broadband links) and connect these into PSN via a gateway and these can be purchased from a wide range of providers. It isn't possible to give costs as these will vary.

Who will provide my connection?

PSN connections may be provided by any of the PSN-Compliant service providers. You may want to buy connections that are not PSN-compliant (e.g. broadband links) and connect these into PSN via a gateway and these can be purchased from a wide range of providers.

So if I can no longer complete a GCF or GSi CoCo can I still buy consume GCF services?

Yes whilst your GCF CoCo is valid and once you have been awarded a PSN CoCo, you will be able to consume GCF Services. Whilst the GCF and PSN CoCo approaches are very different; they are being accepted as equivalent during the transition phase.

How will the connection be transferred from GCF to PSN?

If you have a connection provided under the GCF that is due for renewal you should complete the PSN CoCo rather than the GCF CoCo. Once certified your connection will then be treated as a PSN connection and on expiry of your GCF service contract you will procure your connection from any PSN Compliant service provider.

Note - We will no longer accept GCF or GSi Codes of Connection (CoCo) from the 1 November 2012. For further details please see the PSNA Notice 1 of 2012 - Migration to PSN CoCo Update.

If your connection is not yet due for renewal but you wish to access PSN services you may do so under the following conditions:

> Your CoCo must be in good standing. That is: Not subject to a Compliance Warning Notice, not under a Limited Authorisation Notice and has no outstanding actions against it.
>
> You must complete and sign Section 4 of the PSN Code Template – Commitment statement for PSN Customers, and Schedule II of the PSN Code Template – Customer Environment

If these criteria are met you may request access to PSN via the PSN Gateway from your current connection provider.

How soon after I get my certificate will I get my connection?

The timescales for your PSN connection are dependent on your procurement. You cannot physically connect until you have a PSN certificate, however you may be able to arrange for your connection to be activated on the day you receive your certificate. You should consult your PSN supplier to determine if this is feasible.

Is annual re-certification and approval required?

What happens to my organisation's existing connection if the PSNA does not approve the CoCo?

What happens if my CoCo lapses?

What happens if we don't complete a PSN CoCo when our GCF CoCo ends?

Certification is an annual requirement to maintain compliance and retain PSN access for both Customers and Suppliers. You should submit your PSN CoCo with all its supporting documentation at least 1 month in advance of the annual renewal. Failure to maintain compliance puts you at risk of disconnection.

If you do not gain certification to PSN you may continue to use your existing connection provided under GCF until it expires, subject to you maintaining compliance with the GCF CoCo. Once your GCF CoCo expires you must gain PSN certification in order to continue to use that connection. If you fail to gain PSN certification on expiry of your GCF CoCo and your GCF contract expires you will not be able to procure further connectivity and will be disconnected from the network.

Where do I go for advice on PSN?

You can get general advice and support from the PSN Programme, and the PSN mailbox. Depending upon the nature of the query this may then be referred to the relevant transition team member or subject matter expert. Further contacts and self help information available as follows:-

- PSN Core Team
    - psn@cabinet-office.gsi.gov.uk
- PSN Documents including Standards
    - **www.cabinetoffice.gov.uk/content/public-sector-network**
- PSN Frameworks Factsheet, Service Descriptions and User Guide
    - http://www.cabinetoffice.gov.uk/content/public-services-network
    - http://gps.cabinetoffice.gov.uk/contracts/rm860
    - http://gps.cabinetoffice.gov.uk/contracts/rm1498
- Compliance document queries
    - psna.compliance@cabinet-office.gsi.gov.uk
- CAS(T) Auditors
    - KPMG - Szu.Ho@KPMG.co.uk; tel 0779 3312756

– LRQA - Phil.willoughby@lrqa.com; tel 024 76882217 or 07824 596624

Will I get the same services under PSN as I had under GCF?

All services currently available under GCF will continue to be available via PSN during the transition period. In the longer term there will be a much wider range of services available under PSN until it becomes the predominant means of delivering services to the public sector. The number of services will continue to grow: to see what is available now look at a list of service providers .

What are the benefits to my organisation of being connected to the PSN?

Detailed information on the expected benefits of PSN can be found in the PSN Benefits Guide.

- Simplify the creation and delivery of cross-cutting public services
- Extract the most value from network and telecoms suppliers and substantially reduce the cost to government.
- Lay the network and telecoms services foundation for the government ICT strategy
- Enable the public sector to exploit the best telecommunication capabilities available to the private sector swiftly and in an agile manner.
- Creation of a secure, agile and compliant networks and telecoms environment
- Enable public service staff to gain access to the data and services they require from any appropriate location

Will there be active monitoring of networks as well as reacting to client raised incidents?

A The PSNA Service Bridge will not undertake proactive network monitoring; this is carried out by suppliers according to contractual agreements there are plans to have a Security Operations Centre (SOC) for the PSN, but this will be implemented in phases over the longer term. Any incidents reported to the Service Bridge by customers or suppliers will be investigated and managed accordingly. The PSNA will normally only deal with cross supplier major incidents and security incidents.

I want to be a PSN Customer - What is the application process?

What documents do I need to submit?

As the PSN Code Template says, PSN Compliance applications, annual resubmissions and general compliance enquiries should be sent via email to psna.compliance@cabinet-office.gsi.gov.uk. Documentation marked up to RESTRICTED may be sent to this address. To send material of higher classification, or in cases where you do not have a means to transmit protectively marked material, please contact the PSNA compliance team at the above address in the first instance. A completed Code must carry the same protection marking as the system which it describes.

All candidate PSN Customers should submit the following material with their initial application, and annual resubmission:

- A completed PSN Code Template, including Schedule II
- Sections 3 & 4 of the PSN Code template, recently signed and scanned, preferably as a 'pdf' file
- A completed Annex B
- An up to date network diagram
- A recent IT Health Check report, plus any necessary action plan to address issues found
- The Remedial Action Plan from your most recent CoCo Assessment, if applicable.

What happens after I have sent in my application?

The PSNA will validate the application to ensure that it contains the necessary information. The PSNA may commission an on-site assessment of your Information Assurance conditions, or verification of the other conditions by an independent party at this point.

If you are selected for an on-site assessment you will be required to provide all the supporting evidence cited in your CoCo, prior to the on-site assessment commencing.

How long does a certificate of compliance last?

Once your application meets the required standard your organisation will be approved for certification and a certificate of compliance valid for one calendar year will be issued. Renewal certificates last for one calendar year from the expiry date of your previous certificate; late submissions do not extend your validation period.

Does the evidence column in Annex B need to be completed for the 'Governance' and 'Service Management' worksheets or simply a statement of Yes or No?

It depends on the type of question – see below:

Declaration requires a simply Yes/No answer indicating acceptance or otherwise of the requirements of the control.

Inspection requires the submission of supporting material showing evidence of compliance with the control or specific information requested by the control.

Applicants should be aware that because certification is an annual process there are a number of controls marked for Inspection that cannot be supported with evidence on initial application; for example security incident reporting for a PSN service. In this case you should indicate that you will comply with the controls but that this is an initial application and that evidence has not yet been collected to support compliance.

How do I answer a SHALL control if I'm not sure that I comply? Can we supply information on mitigation, how do we do this?

All SHALL controls must be answered YES for a successful submission; If you feel that you have mitigation in place that achieves the same end result as that of the original control requirement then you should describe this mitigation, making it clear that these are mitigating controls.
The SHALL control requires a commitment to achieving the conditions; if you feel that you do not fully meet the YES criteria your supporting evidence must detail the extent to which you do meet the conditions, and any remedial action you intend to make in order to comply (including timescales). Be as specific as possible.

We will then assess whether the mitigation is sufficient to support the application, you may be asked to supply a supporting Remedial Action Plan.

In the case of Customer IA Conditions, if a particular condition really does not apply to you and you can demonstrate this, you should respond N/A (not applicable). Customer IA Conditions now follow a Statement of Applicability approach, in line with ISO 27000.

Will I get a PSN certificate / Badge / Logo?

On successful completion of the certification process you will be issued with an electronic certificate in PDF format. Logos are also available on request for use by certified organisations. You can use your certificate number to demonstrate PSN compliance when buying and selling PSN services.

As a supplier I want to provide a number of services to PSN connected customers. Can I get my whole organisation certified and just supply the services my customers want?

No. PSN services are certified on a Service by Service basis, with one Code of Practice (CoP) or Code of Interconnection (CoICo) describing each distinct service, even if they are supplied by the same organisation. Each service you wish to provide requires a separate application.
In practice there is likely to be a degree of overlap between the services. Once you have been certified for one service, subsequent services may well prove less onerous to achieve. This is mainly because you may be able to refer to existing submissions where material is duplicated.

Which version of the CoCo, CoICo or CoP do I need to complete?

The current version of the Code Template, including its Annex B, should be completed. This is used by customers and suppliers as appropriate to build a CoCo, a CoICo, or a CoP.

What is a CoCo, CoICo or CoP?

What is a Deed of Undertakings?

There are different types of Code:

- Code of Connection (CoCo): applicable to PSN Customers
- Code of Practice (CoP): applicable to PSN Service Providers.
- Code of Interconnection (CoICo): applicable to those PSN Service Providers that are Direct Network Service Providers.
- Deed of Undertakings: GCN Service Providers are required to enter into a legally binding Deed of Undertakings (DoU) before they can begin delivering GCN Services.

For PSN definitions, please see the PSN Glossary. For further information, see PSN for Dummies.

I want to provide PSN services, can PSNA provide a Technical Advisor to help with our service application?

I want to consume PSN services, where can I get advice on completing the CoCo?

The PSNA do not have the resources available to provide individual technical advice relating to applications, nor can we provide specific answers to the control requirements, these must be developed in line with your internal risk management processes

For consumers, there are a number of commercial organisations with the expertise to assist in completing the CoCo. Help can also be obtained through one of the regional public sector WARPs. Customers should look for consultants who can provide experience in HMG SPF and ISO/IEC 27001.

Suppliers and consumers should consider the services of a CLAS consultant or those with similar experience. The CESG website has further details on CLAS consultants.

I want to be part of PSN, what's the difference between a PSN Service Provider and a PSN Customer?

Public Sector bodies and commercial organisations can be both, although it is more usual for Public Sector organisations to be PSN Customers and commercial organisations to be PSN Service Providers.

PSN Customers are organisations whose staff are consuming services provided on the PSN.

Following this definition, a commercial organisation connected to PSN that is processing information on behalf of a public sector body is therefore a PSN Customer.

PSN Service Providers are organisations supplying or approved to supply ICT services over the Public Services Network.

Some central government departments that provide information to local authorities can therefore be PSN Service Providers.

For more detailed explanation of exceptional circumstances, such as aggregation and sharing services, please see section 3.3 of the PSN Compliance document.

Where can I get the latest version of the CoCo?

All PSN Standards, including the latest versions of the Code Template, from which you can create your own CoCo are available on the PSN Standards website.

Who should sign the declarations in the Code Template?

PSN Service Providers should complete section 3 of the code template; this should be signed by a person with appropriate authority to commit the organisation to the requirements described e.g. Chief Executive, CIO, IT Director or equivalent.
PSN Customers should complete section 4 of the PSN Code Template; the sections should be signed as follows:

- Section 4.1of the Code Template should be signed by a person with appropriate authority to commit the organisation to the requirements described (E.g. Chief Executive, CIO, SIRO, IT Director or equivalent).
- Section 4.2 should be signed by the person responsible for the maintenance and implementation of the organisation's Information Security Management System (ISMS). This could be their Section 151 officer, SIRO, security manager or other responsible person.
- Section 4.3 should be signed by the SIRO or equivalent for public sector organisations. For private sector organisations this should be submitted unsigned and the PSNA will assist in identifying a suitable signatory as part of the assessment process.

What is a PSN service?

A PSN service is any certified service provided to another organisation over the PSN network. It can refer to bespoke commercial applications or to the use of shared services between organisations. For more information, read the 'What is a PSN Service?' document.

Can I share existing services with other organisations over PSN?

Sharing of non-PSN certified services over the PSN is generally not permitted, however it may be possible provided it falls within the limits set out in section 5.3 of the PSN Compliance document:

- The number of PSN Customers sharing the service (in addition to the PSN Customer providing the service) shall be TEN or less.
- The total number of users sharing the service (in addition to those of the PSN Customer providing the service) shall be ONE THOUSAND or less.

In this case it is permitted for an organisation to share services with a limited number of sites or users without that service being separately certified. The intention of this control is for example to allow organisations such as County Councils to share central services with their associated district councils via PSN.

I want to be a PSN Service Provider - What is the application process?

What is the difference between accreditation and compliance?

What documents do I need to submit?

As the PSN Code Template says, PSN Compliance applications, annual resubmissions and general compliance enquiries should be sent via email to psna.compliance@cabinet-office.gsi.gov.uk. Documentation marked up to RESTRICTED may be sent to this address. To send material of higher classification, or in cases where you do not have a means to transmit protectively marked material, please contact the PSNA compliance team at the above address in the first instance. A completed Code must carry the same protection marking as the system which it describes.
All candidate PSN Service Providers should submit the following material with their initial application, and annual resubmission:

- A completed PSN Code Template, including Schedule II
- Sections 3 & 4 of the PSN Code template, recently signed and scanned, preferably as a 'pdf' file
- A completed Annex B.

The PSNA will then validate the application to ensure that it contains the necessary information. When validated, the PSNA will pass on the application to the Pan-Government Accreditor (PGA), who will contact the service provider and commence the accreditation process by requesting a Risk Management and Accreditation Document Set (RMADS). The PSN Risk Management and Accreditation Reference Document (RMARD) outlines the process for creating an RMADS.

Once the service has been accredited, the PSNA will conduct a final review of your application and, subject to approval from the Operations Director, you will be issued with a certificate of PSN Compliance valid for one calendar year from date of issue that will allow you to connect to the PSN and supply the PSN Compliant Service.

What is The Security Policy Framework (SPF)?

The Security Policy Framework is a set of guiding principles presenting a holistic approach to Information Assurance. Within an organisation bounded by the Security Policy Framework, all systems and services shall be accredited in accordance with CESG Information Assurance Standard 1 & 2.

What evidence is required by a PSN Customer to demonstrate effective information risk management?

Should Local Authorities use The Security Policy Framework (SPF)?

The evidence needed to demonstrate that an effective information risk management process is in place is:

- that it is documented and repeatable, and produces evidence of activity
- that there is a register of information assets
- there is senior board-level accountability for information risk
- risks are owned, and being reviewed regularly by the business
- risks are being assessed and mitigations are being applied
- residual risks are known and accepted by the business

Central Government Departments for whom the Security Policy Framework (SPF) applies are mandated to meet HMG IA Standard No 1, a risk management process, which will assist in understanding information risk, and the classification of information assets.

Please note that CESG emphasise that information risk management is a key part of the compliance process and underpins the IA conditions. If the organisation is carrying out effective and robust risk management then they are likely to be able to demonstrate compliance much more easily than one that is not.

A simplified view for Local Authorities is contained in the Local Public Services Data Handling Guidelines.v2.

What guidance is available to help with physical security?

Customers should follow CPNI Physical Security Guidance from the Centre for the Protection of National Infrastructure.

Do existing users require evidence of Baseline Personnel Security Standard (BPSS) compliance?

Must BPSS be applied retrospectively?

Baseline Personnel Security Standard (BPSS), or equivalent, must be implemented for all new starters in line with HR good practice.

BPSS is closely aligned with recognised good practice such as BS7858, and requires:

- Proof of identity and address
- Details of education and employment
- Criminal records check
- Financial check
- Checking of at least two character references

For Scottish Local authorities see Disclosure Scotland.

If your organisation is not using BPSS or equivalent it must instigate a system for all staff that will use PSN now. This process needs to be continuous, though a 3 year plan may be acceptable.

Do staff require regular user education updates?

Yes. These should meet HR good practice guidelines – annually is a good minimum frequency for staff training or education.

Evidence may also include a signed agreement from staff for Acceptable Use Policy (AUP). An example User Acceptance Policy available in PSN IA Condition Supporting Guidance

What incident response processes exist for PSN?

What security incident response processes exist for PSN?

The general principles of PSN incident management are:

- Organisations are responsible for their own incident management processes.
- The PSN Authority gets involved in incidents **only** when contractual responsibilities are not clear, for example when an end-to-end service is provided by more than one Service Provider, outside a Customer's contractual chain.
- Major Incidents that the Service Provider is unable to resolve within its own Service Level Agreement must be escalated to the PSN Service Bridge
- The PSN Authority Service Bridge is a means by which stakeholders who are not necessarily in contractual relationships can communicate quickly
- The PSN Service Bridge does not undertake proactive network monitoring. This is for suppliers to carry out according to contracts with customers.
- A future enhancement to PSN, the SOC (Security Ops Centre) will provide proactive security monitoring.
- Serious security incidents should be reported to GovCERTUK immediately; where the incident directly affects the PSN service or connection your PSN service supplier must also be informed.
- As a matter of good practice, lessons learned from security incidents, should be shared with the regional public sector WARP.

Is there guidance on Configuration e.g. around patching and malware?

Do we need to patch all hardware & software?

Is it acceptable to use only one malware product as protection?

A vast majority of security threats exploit vulnerabilities for which a patch or work-around already exist. To mitigate against this there should be regular monitoring for vulnerability alerts (e.g. through monitoring of relevant information sources/WARP membership) and systematic and regular

patching of all aspects of an ICT system, including operating system, infrastructure firmware and bespoke software applications.
Malicious code or software (commonly known as 'malware') also presents a significant risk to organisations, their ICT systems and information. Malware can be introduced into ICT systems via applications, network interconnections, removable media and attached devices. It is good practice to use multiple anti-malware products, e.g. one on the gateway and another on devices.

Patching and malware protection are critical elements of risk management and are explicitly required for PSN compliance. Evidence of inadequate patching/malware protection will typically be detected as part of the IT Health Check and could jeopardise timely PSN compliance.

Patch Management and Malware Protection requirements are contained in the PSN Code Template Annex B, with further guidance available in the IA Conditions Supporting Guidance. New Patch Management and Malware Protection standards, providing further guidance and recommended controls for consumer organisations and their service providers are now available - Common Standards for Patch Management & Malware Protection .

Is there guidance around the required scope of an IT Health Check (ITHC)?

Are penetration tests sufficient?

Do we need to change our ITHC supplier annually?

A properly scoped IT Health Check covers a number of aspects in addition to a penetration test. Penetration tests alone are not sufficient.
In broad terms the scope of the health check should cover all those systems and networks within the client environment that have or will have access to the PSN network or PSN services. This includes mobile and remote devices such as Tablets, Blackberries, Smartphones, laptops used by remote workers etc. Where appropriate it should also cover the IA requirements listed in the PSN Code Template Annex B.

The ITHC should include an intelligent summary of the findings and recommended actions and timescales, and not simply be a dump of the output from the tools used to conduct the check.

The scope and detail of an ITHC, should be proportionate to the organisation. The CESG Standard for IT Health Checks is CHECK. For IL2 services, organisations do not need to use a CHECK company; however those undertaking ITHCs should be TigerScheme or CREST qualified organisations.

Changing your ITHC supplier annually is good practice, but generally not essential. The key is to get a thorough independent test carried out, which produces a clear meaningful report and action plan, appropriate to the organisation.

An alternative to rotating your ITHC supplier would be to use a different tester each year from the same supplier, or alternate testers.

Is it OK to share accounts?

PSN Customers should apply additional controls when sharing accounts to ensure individuals remain accountable. An audit log of when/how/who accessed account may be sufficient. A rationale, presenting the risks and benefits of sharing accounts should be prepared.

Do we need to describe how removable media is used?

PSN Customers must state what safeguards are in place to mitigate risks. Customer must have a policy and have it incorporated into User Education programme.
More information for Local authorities is available at Local Public Services Data Handling Guidelines.v2 for further information.

Is there a PSN policy on Bring Your Own Device (BYOD)?

Should mobile devices have 2-factor authentication?

Can I connect to PSN using my home PC?

The security around Bring Your Own Device (BYOD) is being developed as part of the Government End User Device Strategy. The key thing is to ensure is that corporate security policies are applied as necessary to the device.
Where possible technically, all mobile devices connected to PSN should have 2-factor authentication.

What is the guidance around access to public wireless networks e.g. captive portals in airports, internet cafes or other public buildings?

Typically, this is not acceptable on PSN because such access points prevent the user from forming an end-to-end encrypted connection between the user and their organisation's core network.
If the user is required to authenticate/connect to a public WiFi portal before making any end-to-end encrypted connection then this is not acceptable.

If an end-to-end encrypted connection can be made without authenticating/connecting to a public WiFi portal, then this is acceptable. However, In addition users should not be able to access an untrusted network such as the Internet directly. Access should be via the organisation's core infrastructure.

What evidence is required for network obfuscation?

Acceptable evidence for network obfuscation includes highlighting the use of Network Address Translation (NAT) and/or Port Address Translation (PAT), or putting in place measures to limit the information available from the network, i.e. prevention of banner grabbing or details of operating systems and versions being used. This should be tested as part of the ITHC.

Are there exemplar network diagrams available to support a PSN CoCo submission?

Is there any guidance around the assurance mechanism for boundary controls?

As a Customer, we will have multiple PSN connections at different impact levels. Can we submit one PSN CoCo for all these environments?

The PSN team are currently working on producing example diagrams and the configuration of boundary controls such as Internet gateways, but unfortunately these are not available at the moment.
CESG produce a number of architectural templates, these are available through the CESG IA Policy Portfolio, available to CLAS consultants.

If you have multiple PSN connections, the number of CoCos you submit is a design decision driven by how simply and accurately your ICT environment can be presented for assessment. A single CoCo may eliminate duplication of paperwork, but may make assessment difficult, and slow down the overall assessment should your environment support higher impact levels.

Any CoCo, or set of related CoCos must clearly show how you are protecting IL4 from IL3 and IL3 from IL2/0. It should also show all physical connections, including connections GSi, xGSi, DWP, swiftnet, BACS etc.

With the PSN there will be networks with multiple sites and multiple connections with cryptographic overlays at different levels. There will therefore be a lot more virtualisation, and networks should show more than just physical connections.

The ultimate authority for this is the Public Sector Accreditation Board, who may decide to reject a Compliance application or renewal if the information presented is not clear.

PSN specifies MPLS interconnects, is MPLS a mandatory requirement for provision of service to PSN customers?

No. PSN obligations for DNSP to GCN Network to Network interfaces are indeed for MPLS NNI's. These are obligations on service providers to ensure the network to network interfaces are fully interoperable. There is no technical specification or requirement on the service offered to customers at the customer network edge (for DNSP's or SP's). The inter network interfaces are mandated for DNSP to GCN and GCN to GCN but the interfaces from network SP/DNSP to customer are not

specified by PSN. PSN envisages a range of interfaces and network services to suit customer needs including variations on the 802.1** IEEE standards. PSN's requirement is that any service provided should be compliant from a security accreditation viewpoint and that at some point the SP or DNSP maps the service to the core MPLS service so that the NNI MPLS interoperability standards are complied with as the service transits the DNSP- GCN interconnects.

It should be noted where a service is not reliant on a virtual separation any suitably security accredited access service is acceptable however, where an IL2-2-4 service is separated from a non accredited service by a logical separation (such as addressing) it is advisable to review the capability of the technology with CESG in respect of security separation prior to accreditation. MPLS has been accepted by CESG as a suitable separation for IL2-2-4 from an un-assured network but that does not mean it is the only viable solution. As things stand it is expected that appropriately compliant IPSec or other solutions are used for assured separation of IL3-3-4 environments from either IL2-2-4 or indeed un-assured networks.

This means that for IL2-2-4, 802.1 aq based Shortest path bridging and other Ethernet base solutions are potentially acceptable solutions for customer services , subject to solution accreditation for the specific implementation.