CESG Architectural Patterns

Walled Gardens for Remote Access
**Purpose & Intended Readership**

This architectural pattern is intended to assist system integrators and accreditors undertaking work for HMG on HMG systems by:

- Raising awareness of efficient, secure solutions to commonly raised business requirements.
- Building an understanding of the capabilities and limitations of the architectural pattern in the context of a wider system.
- Identifying the role of and requirements placed on each component of the architectural pattern.

**Assurance**

Adherence to the principles set out in an architectural pattern does not automatically result in a secure system. It remains the role of the accreditor in collaboration with the system integrator, to satisfy themselves that the realisation of this architectural pattern and the implementation of each component is appropriate to the context in which it is deployed.

CESG provide a range of services that may be used to inform this process.

**Summary**

This pattern describes a standard architecture for providing remote access. It is based on a ‘Walled Garden’ concept. This is where services required by endpoints are presented within a protected zone. This concept helps to ensure that a compromised remote endpoint is limited in the damage it can inflict on a system.

This architectural pattern sets out key design principles to enable a business to expose applications to remote endpoints without giving those endpoints full access to the core network.

It is intended for system integrators and accreditors building Remote Access Solutions (RAS) for HMG on HMG systems.

This document provides only guidance (not mandatory Policy), however in order to claim that you are adhering to a Walled Garden architecture all ‘must’ statements need to be adhered to.
Contents

Chapter 1 - Scope ......................... 3
  Business Scenario ....................... 3
  Pattern Overview ....................... 3
  Assumptions .......................... 4
  Policy and Guidance .................. 4

Chapter 2 - High-Level Overview ..... 5
  Architecture ........................... 5
  Security Considerations .............. 5

Chapter 3 - Access Layer ......... 6
  Function ................................ 6
  Security Considerations .............. 6

Chapter 4 - Presentation Layer .... 8
  Function ................................ 8
  Security Considerations .............. 8

Appendix A – Accreditors’ Notes .. 10
  Accreditors’ Notes ..................... 10

References ............................. 11

Glossary ............................... 12
Chapter 1 - Scope

Business Scenario
1. This architectural pattern is intended to enable access to a subset of business services from managed remote endpoints.

Pattern Overview
2. By constraining the access available to endpoints and users to specific services and subsets of information within the core business network, the impact of a compromised remote endpoint can be limited.

3. This approach of separating remote endpoints from the core is encouraged, as less trust can often be placed in a remote endpoint than the core infrastructure. It also has the benefits of limiting the damage a compromised endpoint can cause and the data that it has access to.

4. Table 1 below identifies the principle risks, controls and residual risks associated with this architectural pattern.

<table>
<thead>
<tr>
<th>ID</th>
<th>Risk</th>
<th>Control</th>
<th>Residual Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A compromised endpoint mounts a network level attack on the core network.</td>
<td>Communications protocols are terminated within the Presentation Layer.</td>
<td>Compromise of the Presentation Layer could enable an attacker to attack the core network. The scale of this risk will be determined by the network controls placed between the presentation layer and core network.</td>
</tr>
<tr>
<td>2</td>
<td>A compromised endpoint mounts a content bound attack on the core network.</td>
<td>Content types are limited by the Presentation Layer and should be filtered and inspected.</td>
<td>Content inspection is not a perfect technology and there remains a residual risk that attacks could pass through this defence.</td>
</tr>
<tr>
<td>3</td>
<td>A compromised endpoint exfiltrates data from the core network.</td>
<td>The data the endpoint has access to is limited by the Presentation Layer.</td>
<td>Some data will still be available through the Presentation Layer to support the business functions. Access to data should be granted based on a business requirement and the risks balanced against the benefits.</td>
</tr>
<tr>
<td>4</td>
<td>The confidentiality or integrity of the communications</td>
<td>The communications are protected with an approved VPN.</td>
<td>Please see the guidance for the VPN product for any residual risks.</td>
</tr>
</tbody>
</table>

Table 1
with the endpoint is compromised.

| 5 | An unauthorised endpoint or user connects to the presentation layer. | The endpoint and user are both authenticated. | The credentials could be compromised. |

Table 1 – Controls and Residual Risks

Assumptions
5. The core network is accredited in line with HMG policy.
6. The remote endpoint is accredited in line with HMG policy to store and process material to the Business Impact Level of the data and services it will have access to.

Policy and Guidance
7. This architectural pattern is supported by CESG guidance on remote access, contained in CESG Good Practice Guide No. 10 (GPG10), Remote Working (reference [a])
Chapter 2 - High-Level Overview

Architecture

8. The architecture is split across two distinct layers, an Access layer that provides access to the system from authorised users and endpoints, and a Presentation Layer that presents a limited view of the core system services. Figure 1 shows a high level view of the architecture.

9. The Access Layer is described in detail in Chapter 3 and the Presentation Layer in Chapter 4.

Security Considerations

10. The security objective of the Access Layer is to protect the system and its communications with the endpoint form the untrusted Wide Area Network (WAN). This layer is responsible for authenticating devices and terminating the encryption.

11. The security objective of the Presentation Layer is to restrict the services that a remote client can connect to, and prevent a malicious remote endpoint or user from directly attacking services on the core system.

12. It should not be possible to bypass a component of the architecture, for example by circumventing the Presentation Layer to reach the core system directly from the Access Layer. To support this goal the Access and Presentation Layers would typically be implemented on physically separate components.
Chapter 3 - Access Layer

Function

13. The role of the Access Layer is to:
   - Terminate any encryption used to protect the link
   - Authenticate the remote user and the end point
   - Provide access to services permitted for that particular user and end point combination

14. The remote user and endpoint must both be authenticated, and the authentication should be tied together so a user can only use their assigned endpoint.

15. The degree of access control granularity will vary from solution to solution and is based on the business requirements. Some solutions will have a single set of services that are accessible to all remote users (and hence be very simple in design), others will require more complex authentication and authorisation solutions to enable different remote users to access specific services. Which services the user and endpoint can access will depend on the rules enforced within the access layer.

Security Considerations

16. The Access layer must authenticate clients and terminate the cryptographic link (referred to as a VPN within this document) connecting the Presentation Layer network with the endpoint. This VPN must be appropriate for the impact level of the services being exposed to the device as stipulated by HMG IA Standard No 4 (IS4), Protective Security Controls for the Handling and Management of Cryptographic Items (reference [b]) and CESG guidance. Depending on the impact level this may entail the use of CAPS approved cryptography, a CESG Manual T (reference [c]) or V (reference [d]) solution or another appropriate solution as approved by the systems accreditor.

17. The Access layer must also provide controls against network level attack from the un-trusted WAN, this type of protection may be included as part of the VPN device or it may require a separate device such as a firewall. The use of a firewall reduces the attack surface of the solution by ensuring that only VPN traffic can reach the gateway. This may not be required in all situations but does help defend the device and is useful in responding to denial of service attacks, Figure II shows this. CESG assured VPN products will have information as part of the configuration guidance on whether a firewall is required and how it should be configured in conjunction with the VPN endpoint.
18. A common configuration when deploying Access Layers involves placing the VPN gateway in a DMZ by utilising a third interface on the firewall (as shown in Figure 3). However this is not recommended where the firewall carries a lower level of assurance than the gateway. Should a vulnerability in the firewall be discovered, it could enable an attack to bypass the VPN gateway.

19. The Access Layer may also provide controls against the risk of network bound attacks on the availability of the system, often referred to as denial of service attacks. Such defences may include advanced features within the firewall, load balancing systems or other Denial Of Service (DOS) protection devices.

20. Controls should be in place to stop different remote endpoints communicating with one another unless explicitly required by a business application.
Chapter 4 - Presentation Layer

Function

21. The functional purpose of the Presentation Layer is to present a subset of enterprise services to the endpoints.

22. Controls must be in place that limit the services within the core network that can be accessed by remote endpoints through the Presentation Layer. This is to minimise the exposure of those services from the endpoints, which by their very nature are more vulnerable to attack.

23. Wherever possible, the solution should attempt to provide a layer of abstraction between the remote endpoint and the central services, however, it is recognised that this is not possible in all environments.

Figure 4

24. Figure 4 shows a typical Presentation Layer for a remote access solution, in this case consisting of three servers that each present a different set of services to the remote clients. The first is a reverse proxy that is used to make internal web based applications available. As a reverse proxy it is used to defend the internal services by authenticating remote users and ensuring they can only access appropriate parts of the intranet and web based applications. The second machine is used as a mail gateway for external machines and the third is a thin client server that is used to make internal, non web based applications accessible.

Security Considerations

25. The Presentation Layer is as a security boundary between the remote and core domain.
26. The Presentation Layer provides a control for the risk of a network bound attack on the enterprise network from a compromised remote endpoint. Where possible, the endpoints should not connect directly to services on the core network, with all communications protocols being terminated at the Presentation Layer. Where endpoints do directly connect in, their access is restricted to the relevant services by a layer 3 firewall.

27. Additional export and import controls are required on this boundary in the following situations:
   - There is a significant threat from the remote endpoints or their users
   - The core network also contains services and data that operate at a higher Business Impact Level than those exposed through the walled garden
   - A service accessed from the endpoint holds a large amount of data, compromise of which would have a greater Business Impact Level due to aggregation
Appendix A – Accreditors’ Notes

Accreditors’ Notes

28. There is a residual risk of a compromised endpoint compromising the confidentiality, availability or integrity any data that it legitimately has access to. This is the same as with any remote access solution and is why the device should be protected appropriately to the requisite Business Impact Levels for the information it is required to store and process.

29. Where complex data formats parses between the remote endpoint and the core network, there is risk of an attack on the core network from the endpoint. This may be reduced using technology such as content filtering but is hard to eliminate completely. Assurances may need to be sought as to how applications on the core network accept input from the gateway, particularly when this input is generated on the remote endpoint (even if through an intermediary).

30. This pattern is applicable to networks processing data at all impact levels.

31. There may be other residual risks, following this design pattern does not negate the need for a normal risk assessment.
References

Unless stated otherwise, these documents are available from the CESG website. Users who do not have access should contact CESG Enquiries to enquire about obtaining documents.


[b] HMG IA Standard No. 4, Protective Security Controls for the Handling and Management of Cryptographic Items (OFFICIAL SENSITIVE) – latest issue available from the CESG website.


# Glossary

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIL</td>
<td>Business Impact Level</td>
</tr>
<tr>
<td>CAPS</td>
<td>CESG Assisted Product Service – A formal scheme run by CESG for bringing assured cryptographic products to the government market</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarised Zone</td>
</tr>
<tr>
<td>Managed Remote Endpoint</td>
<td>A device used for remote access that is under administrative control of the enterprise</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
</tbody>
</table>
CESG provides advice and assistance on information security in support of UK Government. Unless otherwise stated, all material published on this website has been produced by CESG and is considered general guidance only. It is not intended to cover all scenarios or to be tailored to particular organisations or individuals. It is not a substitute for seeking appropriate tailored advice.