VPN Authentication

ABC

EDS Confidential

Project Id:	IPSec VPN
Document Id:	PE-TAS030002
Cross Ref:	
Version:	0.c
Status:	Draft
Date:	4th April, 2005
Author:	David M. Wozny

CONFIDENTIALITY

The descriptive materials and related information in this document contain information that is confidential and proprietary to EDS®. This information is submitted with the express understanding that it will be held in strict confidence and will not be disclosed, duplicated or used, in whole or in part, for any purpose other than evaluation of this document.

ACKNOWLEDGEMENTS

- Microsoft® is a registered trademark of Microsoft Corporation.
- Windows™ is a registered trademark of Microsoft Corporation.

NOTICE

All versions of this document not labelled **FINAL** are subject to change without notice and should not be construed as a commitment by EDS.

EDS assumes no responsibility for errors or representation that may appear in versions of this document not labelled **FINAL** on the title page.

This document conforms to EDS documentation standards specified in Ref [1].

Text in the document which is grey highlighted indicates that the section is incomplete.

Authors

The accredited author of this document is *David M. Wozny* of EDS.

Enquiries To

Any enquiries should be directed to the author.

Revision History

Version	Date	Status	Description of Revisions
0.a	14th February 2005	Draft	First Draft for Peer Review
0.b	18th February, 2005	Draft	Draft for EDS Tower Review
0.c	4th April, 2005	Draft	Draft for Customer Review

References

No.	Ref.	Title	Ver.	Date	Author
1	PRDA9000	Documentation Standards	1.1	5th April 02	Howard Gladwyn
2	TDU-HLD-001	ABC Remote and Mobile	1.1	18th October, 2004	Alistair Harris
3	PE-TAS030001	Certification Authority Services	1.0	11th February, 2005	David Wozny

Table of Contents

Table of Figures

Table of Abbreviations

3DES	Triple (Round) Data Encryption Standard
ACL	Access Control List
AD	(Microsoft) Active Directory
ADSL	Asymmetric Digital Subscriber Line
API	Application Programming Interface
CA	Certification Authority
CDP	CRL Distribution Point
CM	(Microsoft) Connection Manager
CRL	Certificate Revocation List
DMZ	De-Militarised Zone
DOS	Denial of Service
DR	Disaster Recovery
DSMC	Distributed Systems Management Centre
EAP	Extensible Authentication Protocol
EKU	Enhanced Key Usage
FQDN	Fully Qualified Domain Name
GDP	Group Desktop Program
GPO	Group Policy Object
HTTP	Hyper-Text Transfer Protocol
HA	High Availability
HLD	High Level Design
IAS	Internet Authentication Service
ICS	Initial Connection Services (Zone)
IPSec	IP Security
ISA	(Microsoft) Internet Security and Acceleration Server
L2TP	Layer 2 Tunnelling Protocol
OID	Object Identifier
OU	(LDAP) Organisational Unit
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial In User Service
SA	(IPSec) Security Association
VPN	Virtual Private Network
WWW	World Wide Web

1 INTRODUCTION

1.1 Background and Purpose

EDS Production Engineering – Client Engineering has been engaged by ABC to supply a managed service delivering an L2TP/IPSec VPN solution over ADSL to provide ABC staff with access to services hosted on the new GDP estate.

The agreement provides for EDS to design, implement and manage the proposed VPN solution on behalf of ABC.

This document is governed within the solution framework mandated in the ABC Remote and Mobile High-Level Design, see Ref [2].

1.2 Objectives

This document presents the proposed machine and user authentication design for the ABC IPSec VPN solution. The design is heavily influenced by two principle requirements mandated by ABC:

- Machine authentication by means of digital certificates;
- Strong (two-factor) user authentication by means of the RSA SecurID product.

1.3 Scope of Work to be Provided

The document covers the following scope:

- Digital Certificates
  - Required certificates and enrolment mechanisms / procedures
  - Certificate revocation checking
- RADIUS Server Infrastructure Design
  - Design and placement of IAS servers
  - IAS server load balancing and availability
  - Configuration and rules for user authorisation
- SecurID Infrastructure Overview
  - Discussion of the infrastructure elements required to support the SecurID token solution
- VPN Client Configuration
  - Connection manager configuration
- GDP Impact
  - The wider design implications of user authentication for the VPN project, such as effect on group policies, security groups, etc.

1.4 Scope of Work to be Excluded

This document covers only the scope specified in Section 1.3 above. Without limiting the foregoing, the following items are specifically outside the scope of work:

- The certification authority infrastructure supporting the issuance of certificates, see Ref [3] for further information
- Design of the RSA Authentication Manager infrastructure employed to support the SecurID tokens

- Design of the directory synchronisation between Active Directory and the RSA Authentication Manager
- Processes supporting the issuance of SecurID tokens
- The interaction of the CM with any proposed unified dialler
- The deployment of the CM profile (connectoid)

Access level controls such as Kerberos tickets and Active Directory security groups, etc. are for the purpose of this project considered to be available in the underlying GDP deployment and therefore do not need to be addressed in this document.

1.5 Assumptions

- There is no existing implementation that represents a constraint on this design
- A certification authority infrastructure based upon Windows Server 2003 is implemented to support all necessary certificate requirements for user authentication
- The VPN client software will be the Microsoft Connection Manager
- The VPN concentrator will be Microsoft ISA Server 2004
- Two-factor user authentication will be facilitated by RSA SecurID
- RSA Authentication Manager infrastructure will be provided by ABC and is at version 6.0
- The product selected to perform the user authorisation is Microsoft Internet Authentication Service

Note: References to AD security group names made in this document are for illustrative purposes only, actual names will be assigned by DSMC

2 OVERVIEW OF VPN AUTHENTICATION AND AUTHORISATION

2.1 Introduction

Authentication for the VPN project consist of two main streams:

- Machine Authentication
- User Authentication

2.1.1 Machine Authentication

Machine authentication involves the VPN client software engaging the IPSec driver to submit a signed authentication request and valid certificate to the VPN concentrator; and likewise, the VPN concentrator submitting a signed authentication request and valid certificate to the VPN client (mutual authentication). All client computers participating in the IPSec VPN project will enrol for a client authentication certificate by means of group policy auto-enrolment capability.

2.1.2 Two Factor User Authentication & Authorisation

Authentication and authorisation is achieved via a combination of RSA SecurID tokens and remote access policies managed by the IAS service.

1. Authentication

   Users will be required to possess an RSA SecurID token that generates a unique token code that changes every sixty seconds (something you have) and a PIN code (something you know). The SecurID authentication process demands that the user submits to the VPN concentrator a pass-code, which is a combination of the token code and PIN code.

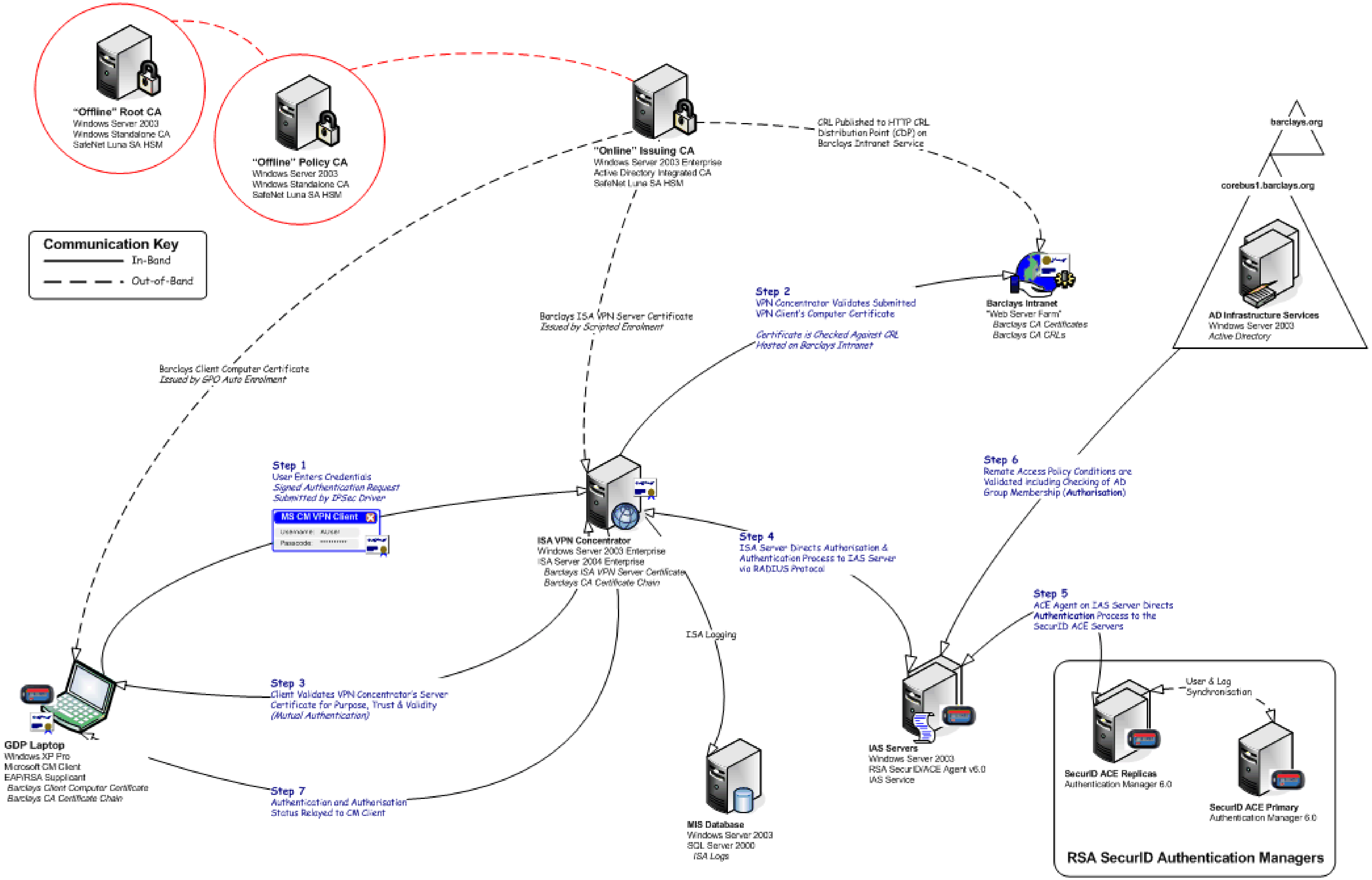
2. Authorisation

   IAS will facilitate Windows integrated user authorisation by means of remote access polices.

ISA VPN concentrators will be configured to forward RSA Security EAP authentication payload using the RADIUS protocol to one of two IAS servers situated in the ICS zone. As well as hosting remote access policies to support user authorisation, SecurID authentication agents will be installed on the IAS servers to “intercept” the RSA Security EAP authentication process and direct it to the appropriate RSA Authentication Manager servers which will also be hosted in the ICS zone, see Ref [2]

Each of the elements involved in the authentication process will be deployed in a highly available configuration to mitigate against the failure of any single component.

Figure 1 on the following page shows a high-level overview of the VPN authentication process.



Step 1
User Enters Credentials
Signed Authentication Request Submitted by IPSec Driver

Step 2
VPN Concentrator Validates Submitted VPN Client's Computer Certificate

Certificate is Checked Against CRL Hosted on Barclays Intranet

Step 3
Client Validates VPN Concentrator's Server Certificate for Purpose, Trust & Validity
(Mutual Authentication)

Step 4
ISA Server Directs Authentication & Authentication Process to IAS Server via RADIUS Protocol

Step 5
ACE Agent on IAS Server Directs **Authentication** Process to the SecurID ACE Servers

Step 6
Remote Access Policy Conditions are Validated including Checking of AD Group Membership (**Authorisation**)

Step 7
Authentication and Authorisation Status Relayed to CM Client

Figure 1 - Overview of VPN Authentication Process

2.2 Authentication and Authorisation Sequence “Walkthrough”

Step One

i) The user initiates a VPN connection by double-clicking on the CM connectoid and entering their username and SecurID pass-code.

ii) The IPSec driver on the client signs an authentication request with the client’s authentication private key and submits this along with the client’s authentication certificate to the ISA VPN concentrator.

Step Two

i) The ISA VPN concentrator validates the authenticity of the signed request against the client’s public key which is presented in the client’s certificate.

ii) The ISA VPN concentrator validates the client’s authentication certificate for chain of trust, purpose, date currency and verifies that the certificate has not been revoked by comparing the serial number in the certificate against the list of revoked certificates in the CRL of the CA server that issued the certificate. The CRL is “hosted” on an HTTP distribution point located in the ABC corporate TCP/IP network, the CRL is cached by the ISA VPN concentrator for the validity period of the CRL, which is seven days.

Step Three

i) The ISA VPN concentrator signs an authentication request with it’s server authentication private key and submits this along with it’s server authentication certificate to the client.

ii) The client validates the server’s authentication certificate for chain of trust, purpose and date currency. The client does not attempt to perform a CRL check against the server’s certificate as there is insufficient network connectivity at this stage to achieve this.

Providing all of the certificate validation checks have completed satisfactorily, the IPSec SA main mode (sometimes referred to as phase one or aggressive mode) completes. IPSec quick mode (sometimes referred to as phase two) is then initiated to negotiate a set of symmetric encryption keys to facilitate the establishment of a secure channel.

The user credentials entered at the start of the connection initiation are now transmitted from the client to the VPN concentrator within the secure channel.

Step Four

i) The ISA VPN concentrator directs the entire user authentication payload, which uses the RSA Security EAP protocol, to one of the IAS servers via RADIUS protocol.

Step Five

i) The ACE agent on the IAS server converts the authentication payload from RSA Security EAP to a protocol that is supported by the RSA Authentication manger servers.

ii) The ACE agent directs the authentication payload to one of the RSA Authentication Manager replicas hosted in the ICS DMZ.

iii) The RSA Authentication manager replicas validate the authentication credentials and if successful send a success acknowledgement back to the IAS server.

Step Six

i) The user credentials are validated against remote access policy rules on the IAS server. Multiple conditions within the policy rules are evaluated and all must be satisfied for remote access to be granted. Amongst the conditions to be evaluated is the verification that the user account presented in the credentials is a member of an authorised AD domain security group (VPN users); to validate this condition, it is necessary for the IAS server to perform a read operation against an AD domain controller.

Once all conditions are met and profile settings applied (such as session timeouts, etc.) a remote access granted permission is applied to the request – if any of the conditions failed a request denied is applied to the request.

Step 7

The success status is relayed to the client and the VPN session established.

2.3 CM VPN Client

The CM VPN client supports RSA SecurID tokens as a means of user identity validation by employing EAP, which is a method whereby various strong authentication protocols can be used as part of an authentication process; this is opposed to using a password based authentication mechanism such as MS-CHAP v2.

RSA Security EAP is not natively supported in Windows XP base operating system, requiring the installation of the RSA Security EAP supplicant on all participating clients.

The CM VPN client configuration mandating the use of L2TP instructs the IPSec driver to select a certificate from the client's computer certificate store containing the appropriate client authentication object identifier (OID), which in this case will be the ABC Client Authentication certificate issued by group policy auto-enrolment.

2.4 VPN Concentrator

The VPN concentrator selected for this project will be Microsoft ISA Server 2004 running on a hardened Windows Server 2003 platform in the context of a Celestix MSA4000 appliance. As a security and management measure, the ISA Servers will be installed into an entirely separate (and untrusted) AD forest to the ABC GDP AD forest.

In terms of participation in the user authentication process, the ISA Servers perform the role of RADIUS clients such that all incoming EAP traffic is simply forwarded to upstream IAS servers to validate the credentials presented.

The ISA Servers will be configured to direct user authorisation requests to one of two IAS servers which will be hosted in the ICS zone. Load balancing of requests will be achieved by alternating the primary and secondary IAS servers to which authorisation requests are forwarded on each VPN concentrator.

2.5 Internet Authentication Service

The role of user authorisation will be performed by the deployment of Windows 2003 servers running the IAS service. The IAS service facilitates the centralised deployment of remote access policies which are integrated into corebus1.ABC.org Active Directory.

The remote access policies will be deployed to enable the requirement of an authorisation attempt to match distinct policy conditions before the request is granted access permission. Typical RAS policy conditions are to specify that the Tunnel-Type is L2TP, that the NAS-IP-Address matches the known IP addresses of the VPN concentrators and that the Windows-Groups matches an AD security group to which the user being authorised is a member of.

In combination with policy conditions, connection profile settings will be applied to authorised users such that idle and connection timeouts are applied as well as mandating 3DES as the compulsory tunnel encryption algorithm.

2.6 RSA SecurID Infrastructure

As discussed in Section 2.4, the VPN concentrators simply perform the role of RADIUS clients and forward authentication requests that they receive (RSA Security EAP in this context) to upstream RADIUS servers which are running the IAS service.

The IAS servers will have the RSA Authentication Agent 6.0 installed and configured to *hand-off* the authentication process to one of two upstream RSA Authentication Manager servers which will be installed in the ICS and be configured in the role of RSA Authentication Manager replicas.

3 MACHINE AUTHENTICATION

3.1 Introduction

All computers participating in the VPN service will posses a digital certificate attesting to the identity of the computer; the IPSec driver on the client generates an authentication request signed by its private key and presents it along with the certificate to the VPN concentrator early in the SA negotiation process as part of the establishment of the IPSec encrypted channel.

The VPN concentrator checks the validity of the signed request, including referencing a CRL. Likewise, further to the VPN concentrator successfully validating the VPN client's identity, the IPSec driver on the VPN concentrator signs an authentication request of its own and presents this along with its certificate to the VPN client; the client checks the validity of this request - although it does not refer to a CRL as it is assumed that network connectivity is not established at this point.

3.2 Certificate Types and Certificate Enrolment

Two types of certificate will be deployed to support machine authentication:

- Server Authentication Certificate for the VPN Concentrator
- Client Authentication Certificate for the VPN Client

3.2.1 Server Authentication Certificate

The issuing CA server deployed into the ABC GDP estate to support the issuance of end-entity certificates will be integrated with GDP Active Directory, this facilitates auto-enrolment of certificates if so desired. However, this support is only enabled for members of the same Active Directory forest. The VPN concentrators being deployed to support the IPSec VPN project will be installed into an entirely separate AD forest than the GDP AD forest which means that auto-enrolment cannot be used. Windows Server 2003 CA services also supports HTTP based certificate enrolment, but again, that is only supported for members of the same AD forest.

Consequently, a scripted means is required to support the enrolment lifecycle of certificates for the VPN concentrators, the following sequence shows a high-level workflow of the server certificate enrolment process:

- Generate a new certificate request on the VPN concentrator (saved to a floppy disk)
- Submit the certificate request to the issuing CA server
- Approve the pending certificate request at the issuing CA server
- Retrieve the issued certificate from the issuing CA server
- Install the issued certificate into the VPN concentrator's certificate store

The server certificate that is issued is based upon a certificate template that is published to the issuing CA server, the key design specifications for the server certificate are included in Appendix A.

The certificate will contain a specific server authentication OID such that it can be used for server identity affirmation purposes.

In addition to the server certificate, the VPN concentrator must also posses all necessary certificates to complete the certificate trust chain up to the root CA level. In practice, this means that the *ABC-RootCA* certificate must be installed into the Trusted Root Certification Authorities certificate store and the *ABC-PolicyCA1* and *ABC-IssuingCA1* certificates must be installed into the Intermediate Certification Authorities certificate store. The installation of these CA server certificates will be via manual processes for the same reasons as specified for the VPN concentrator end-entity certificate.

3.2.2 Client Authentication Certificate

Since all VPN client computers will be members of the same GDP Active Directory forest as the issuing CA server, it is sensible to configure the enrolment of client certificates by means of group policy. Auto-enrolment via group policy requires a combination of two configuration items:

- Configuration of a group policy to enable the following: Computer Configuration \ Windows Settings \ Security Settings \ Public Key Policies \ AutoEnrolment \ Enrol Certificates Automatically. No changes are required to the user configuration part of the group policy and hence user configuration settings can be disabled if so desired.
- Configuration of an ACL on the ABC Client Authentication certificate template to enable the auto-enrolment permission for members of the ABC VPN Computers group.

The client authentication certificate that is issued is based upon a certificate template that is published to the issuing CA server, the key design specifications for the client authentication certificate are included in Appendix B.

The certificate will contain a custom application OID such that it can be used for “wider” client identity affirmation purposes. The custom application OID will not be used in the context of VPN authentication, but would be employed if the certificate was to be used as part of an 802.1x authentication scheme – the inclusion of the custom OID does not affect the VPN authentication, but does remove a level of complexity if ABC decide to employ client-side certificates for 802.1x authentication.

In addition to the client authentication certificate, the VPN client must also posses all necessary certificates to complete the certificate trust chain up to the root CA level. All certificates will be installed into the requisite certificate stores by a GPO initiated process.

3.3 VPN Client Configuration – Subscriber Party

In the context of this project, a subscriber is a computer which has been issued a digital certificate, i.e. the laptop.

No configuration is necessary on the client over and above enrolling for the client certificate and CA server certificate chain as described in Section 3.2.2. Once the properties of the CM connection have been configured to use an “L2TP IPSec VPN” connection, the IPSec driver makes the necessary calls to automatically select the client’s authentication certificate from the computer certificate store based upon the certificate possessing the client authentication OID.

3.4 VPN Concentrator Configuration - Relying Party

In the context of this project, a relying party is a party which accepts a signed authentication request presented by a subscriber for use in a transaction, i.e. the VPN concentrator.

As with the VPN client configuration, little configuration is necessary on the VPN concentrator over and above enrolling for the necessary VPN server certificate and CA server certificate chain.

The single design consideration that must be specified is for the VPN concentrator to “Verify that incoming client certificates are not revoked”, this setting is made under the *Specify Certificate Revocation* general configuration settings on the ISA server management console.

The ISA server will retrieve the CRL via the HTTP CDP specified in the subscriber’s certificate, therefore, the necessary ports and routes must be opened between the VPN concentrator and the HTTP CDP which will be hosted on the ABC corporate TCP/IP network. The HTTP CDP is located in the ABC corporate TCP/IP network (rather than in the ICS DMZ) as there may be other future applications which may need to access the CRL published by the issuing CA which do not have necessary connectivity to the ICS DMZ.

4 USER AUTHORISATION – IAS

4.1 Introduction

IAS servers will be deployed in the ICS zone to support user authorisation; the servers will be members of the corebus1.ABC.org Active Directory domain. Two servers have been specified for high availability – the load generated on the IAS servers by the number of users participating in the VPN project can, if required, satisfactorily be handled by a single IAS server. Incoming authorisation requests will be validated against a remote access policy configured on each of the IAS servers.

Figure 2 shows a high level overview of the authorisation infrastructure; the AD domain controllers shown here represent existing corebus1.barlcays.org domain controller situated within the ABC corporate TCP/IP network.

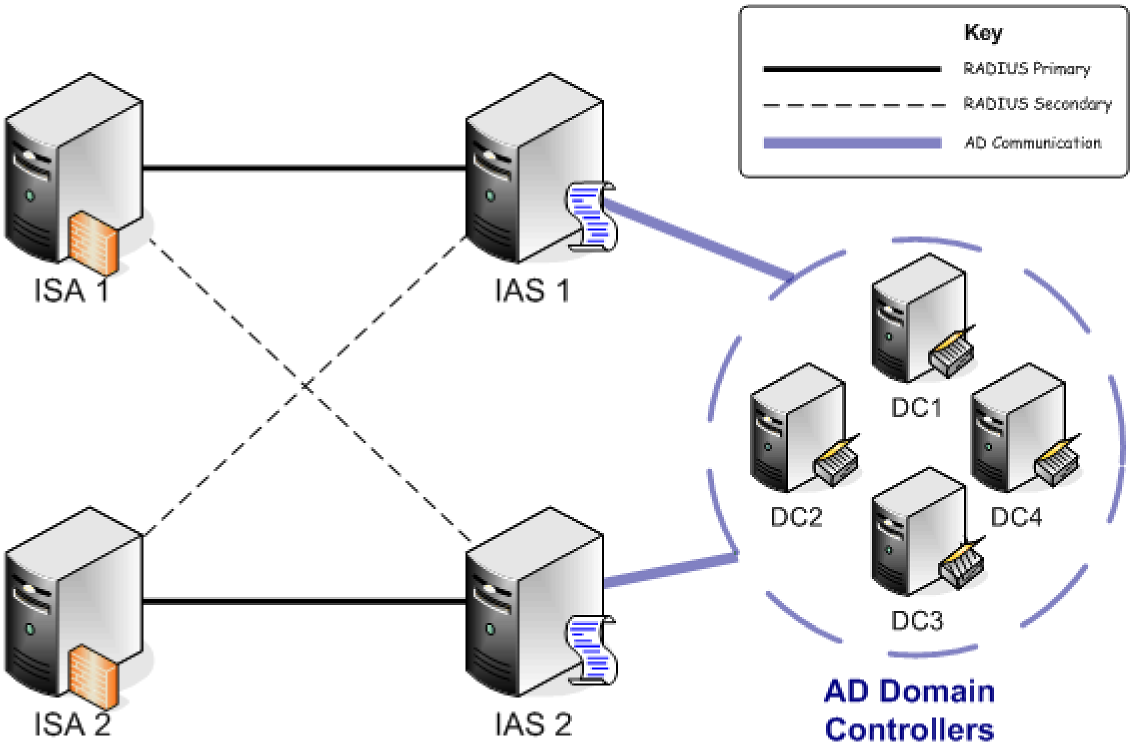


Figure 2 - VPN Authorisation Infrastructure

4.2 RADIUS Configuration

The IAS servers will have RADIUS clients configured that correspond to the TCP/IP addresses of the ISA VPN concentrators, both IAS servers will specify both ISA VPN concentrators as clients. The clients will not require the message authenticator attribute to be set on the either end of the RADIUS client / server pairing as all EAP authentication automatically includes this attribute in the authentication process.

Each RADIUS client / server pairing requires a shared secret to be configured at “each end”, there will therefore be a total of four pairings. The two pairings initiated by the first ISA VPN concentrator will specify one shared secret and the two pairings initiated by the second ISA VPN concentrator will specify another shared secret; the secret will be a twenty character complex string.

The authorisation request presented to the IAS server via the ISA VPN concentrator will not contain a domain identifier in the user logon credentials, consequently the IAS server will automatically pre-pend the domain identifier of the domain of which it is a member (i.e. corebus1.ABC.org) to the user logon credentials; this is default behaviour for an IAS server and therefore needs no specific configuration to achieve this.

4.3 Remote Access Policies

4.3.1 Overview

A remote access policy consists of three main elements:

- Policy Conditions

  Remote access policy conditions are one or more attributes that are compared to the settings of the connection attempt. If there are multiple conditions, then all of the conditions must match the settings of the connection attempt in order for it to match the policy.

- Profile Settings

  A remote access policy profile is a set of properties that are applied to a connection when it is authorized.

- Permission

  If all conditions of a remote access policy are met, remote access permission is either granted or denied.

Remote access policies are specified in an ordered list, if the request matches the first policy in the list then the appropriate permission is applied to the request and further policies are not evaluated. In the event of a request not matching the conditions in the first policy in the list, the request is then matched against the second policy in the list, and so on. In the event of no valid matches against a remote access policy, then an implicit deny remote access is applied to the request.

4.3.2 ABC VPN Remote Access Policies

It is proposed that two remote access policies are employed to support VPN user authorisation. The first policy will contain a list of specific policy conditions and profile settings that a user authorisation request must posses in order for a grant remote access permission to be applied to the request; the second policy will contain a deny remote access permission for all times.

The purpose of the second policy is to ensure that an invalid authorisation request is explicitly denied rather than simply denied as a consequence of not matching a specific rule.

4.3.2.1 ABC VPN Permit

A sample of the policy conditions that must be met include:

- NAS-IP-Address matches “x.x.x.x; y.y.yy”, etc.
- Tunnel-Type matches “L2TP”
- Windows-Groups matches “corebus1.ABC.org\VPN Users”

A sample of the profile settings applied to the policy include:

- EAP-Methods = “RSA Security EAP”
- Encryption = “Strongest” – *Note: for an L2TP VPN this correlates to 3DES*

The permission will be set to Grant Remote Access Permission.

Details of the exact policy conditions and profile settings are included in Appendix C.

4.3.2.2 ABC Deny All

A single policy condition must be met:

- Day-And-Time-Restriction matches “Sun 00:00-24:00,Mon 00:00-24:00”, etc.

The permission will be set to Deny Remote Access Permission.

4.3.3 Remote Access Policy Synchronisation

As either of the two IAS servers could be directed to perform user authorisation, both servers must possess the exact same remote access policies and configuration. To maintain consistency across the two IAS servers it is necessary to use a scripted process to backup the configuration of the “nominal primary” IAS server and restore this to the “secondary” IAS server. The NETSH command that is provided with the base Windows Server 2003 operating system will be used to perform the synchronisation, which will need to be performed at the initial install and at any subsequent time when either policy or configuration changes are mandated.

The proposed approach for deploying the configuration and policies is to develop the IAS configuration and policies in the live-like environment and then export all elements, as listed below:

- IAS Server Settings
- IAS Log Settings
- IAS Remote Access Policies
- IAS Connection Request Policies
- IAS Clients

Subsequently, the elements will be taken to both of the IAS servers to be deployed for the live estate and imported into the IAS service. Subsequent to the imports, it will be necessary to change the shared secrets for the specified RADIUS clients as “dummy” shared secrets will be populated into the configuration in the live-like environment.

4.3.4 Remote Access Lockout

Remote access account lockout policy is used to specify how many times a remote access authentication can fail against a valid user account before remote access is disabled for the user; remote access lockout is a distinct lockout policy from the AD domain user account lockout policy. Remote access account lockout is especially important for VPN connections over the Internet since an attacker on the Internet could launch a denial-of service attack by sending credentials (valid user name, guessed password) during the VPN connection authentication process. If remote access lockout is not specified, an attacker with possession of a list of user names could quickly disable potentially thousands of user accounts in a single attack.

There are two principle settings (which are applied at the IAS server) that apply to remote lockout:

- MaxDenials – the number of failed attempts before future attempts are denied.

  Best practice dictates that this should be set to one less than the domain lockout policy, which for corebus1.ABC.org is set to three; hence the MaxDenials proposed for the IAS servers is two.

- ResetTime - the frequency with which the failed attempts counter is reset.

  It is proposed to assign the ResetTime a value of five minutes - meaning that a DOS attack would be thwarted, whilst the user would not be forced to make a helpdesk call for account re-enabling as a consequence of a genuine mistaken credential submission.

Unlocking an account for remote access before the reset time has elapsed is rather cumbersome, requiring the manual removal of a registry value (which is in the format of *domain:username* in the same location as the MaxDenials registry value) on the IAS server which enforced the remote access lockout. The selection of suitable settings is therefore a balance between security and usability – i.e. avoiding the circumstance whereby the registry entry removal is required.

4.4 Connection Request Policies

Windows Server 2003 IAS servers can perform the role of either a RADIUS server or a RADIUS proxy. In circumstances whereby IAS is required to be a RADIUS proxy, it is necessary to specify a connection request policy to explicitly mandate which requests the IAS proxy is to forward on to an upstream RADIUS server.

In circumstances whereby IAS is required to perform the role of a RADIUS server, which is the case for the ABC IPSec VPN, the default connection request policy to "Use Windows Authentication for All Users" which effectively instructs IAS to use Active Directory integrated authorisation is sufficient. No changes are proposed to the default connection request policy.

4.5 Accounting and Logging

The IAS service has three principle log setting options, for the purpose of the IPSec VPN project it is deemed necessary to log *Accounting requests* and *Authentication requests* – it will not be necessary to log *Periodic status* as these events typically include a lot of "chatter" between the IAS servers to test for availability and include no user data .

The log files will be generated in an IAS format that enables the files to be read by third-party tools which can derive management information from the accounting logs if necessary.

It is proposed that the log files are created on a weekly basis on the IAS servers and are purged on a weekly schedule from the IAS server to a suitable management information repository.

5 USER AUTHENTICATION – RSA SECURID

5.1 Introduction

The RSA SecurID authentication infrastructure employed to support RSA SecurID token based authentication will be provided as a service by *ABC* for the IPSec VPN project to "plug in to"; the availability and performance of SecurID infrastructure is outside of the control of EDS. Further to the IPSec VPN pilot, it is understood that ABC will be inviting tenders for "outsourcing" of the operation of the SecurID service.

There are three main elements involved in the deployment of a SecurID infrastructure in the context of the ABC IPSec VPN project:

- RSA Security EAP Supplicant
- RSA ACE Agent
- RSA Authentication Manager

The EAP supplicant and ACE agent will be installed on devices which EDS control and manage, the RSA Authentication Manager components will be installed, managed and operated by ABC.

Figure 3 shows a high level overview of the authentication infrastructure.

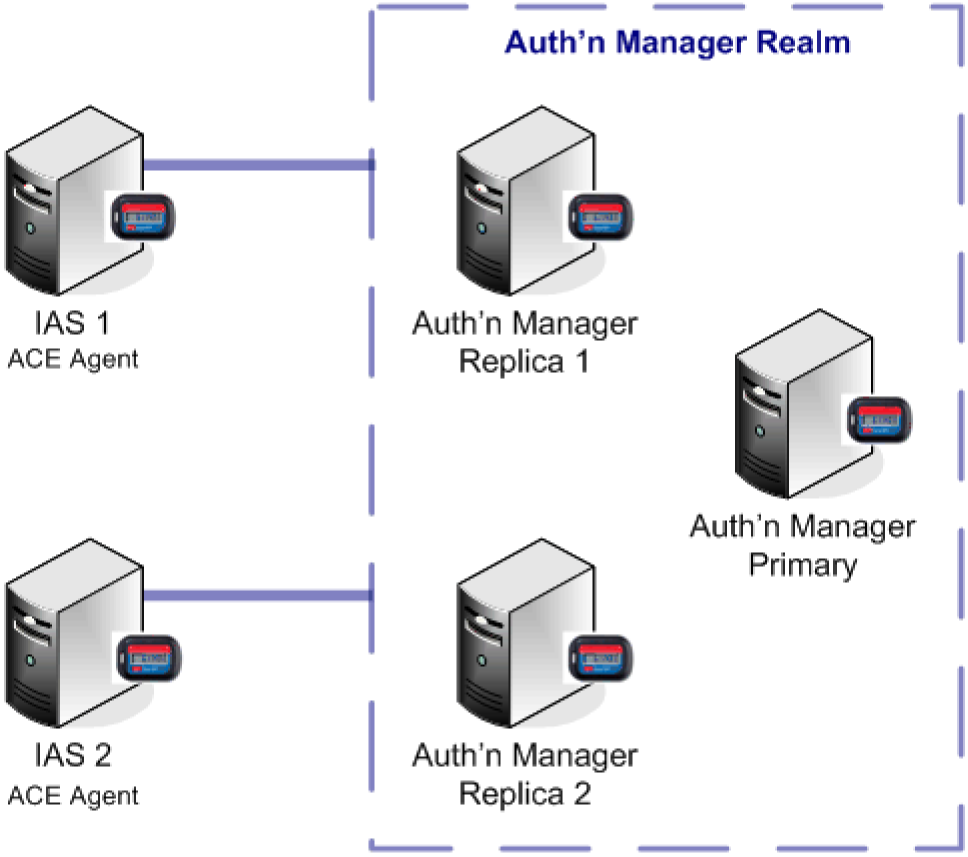


Figure 3 - VPN Authentication Infrastructure

5.2 RSA Security EAP Supplicant

The EAP supplicant will be installed on all laptops that participate in the IPSec VPN project. No configuration is necessary of the EAP supplicant, it is simply referenced as the required EAP type in the advanced security settings of the connection manager connectoid.

5.3 RSA ACE Agent

5.3.1 Overview

To support the use of SecurID tokens as part of the authentication process, it is necessary to install ACE agents on the RADIUS servers - in the case of the VPN project these correlate to the IAS servers. The ACE agent converts the authentication protocol from RSA Security EAP into a protocol that the RSA ACE server supports and then forwards the authentication process to the ACE servers. It is worth noting that the RSA Authentication Manager does not support EAP either natively or in combination with the installation of the RSA RADIUS service for RSA Authentication Manager.

5.3.2 Implementation

As part of the installation of the agent it is necessary to reference an SDCONF.REC file which is generated on the RSA Authentication Manager primary server. The SDCONF.REC file contains the names and TCP/IP addresses of the RSA Authentication Manager servers as well as configuration details – this file will need to be supplied by ABC and is a critical part of the function of the ACE agent. If changes are made to the RSA Authentication Manager infrastructure, it will typically be necessary to re-distribution a new SDCONF.REC file to all ACE agents.

Under normal circumstances, ACE agents operate a load balancing algorithm that involves periodically polling RSA Authentication Manager servers to determine the best path to take when handling an authentication request. To ensure that the ACE agent directs authentication traffic to one of the two Authentication Manager replica servers which are hosted in the ICS zone and not to the Authentication Manager primary server which is hosted within the ABC corporate TCP/IP network it may be necessary to deploy a configuration file, SDOPTS.REC, which over-rides the automatic load balancing algorithm. It will not be possible to determine whether this is required until further details of the proposed ABC hosted SecurID service are made available.

5.4 RSA Authentication Manager

5.4.1 Overview

RSA Authentication Managers (known in previous versions as ACE servers) handle the authentication requests directed to them by the RSA ACE agents. The authentication manager validates the username and PASSCODE presented in authentication requests against its directory of users and tokens assigned to those users.

5.4.2 Implementation

It is understood that ABC will be providing two RSA Authentication Manager servers running as replicas which will be deployed in the ICS zone. The replicas will be read-only and capable only of handling authentication requests and feeding back to the RSA Authentication Manager primary server necessary logging information.

6 IMPACT ON GDP

6.1 Registration

IAS servers are integrated into Active Directory and as such require a user with Domain Administrator privileges for corebus1.ABC.org to register the IAS service with Active Directory; this enables IAS to read user account information from AD.

6.2 AD Security Group Membership

A corebus1.ABC.org security group, ***000000-C1SGG-VPNUserAuthorisation***, will be used to control which users are authorised for the VPN service – only users who are a member of the group have the potential to be authorised by IAS.

6.3 AD User Account Remote Access Attribute

It is understood that all user accounts have the Remote Access Permission attribute set to "Control access through Remote Access Policy" set. If this is not set, it will be necessary to implement an over-ride in the remote access policy.

6.4 Performance / Volumetrics

Whenever an IAS server is called upon to perform a user authorisation, an upstream referral to a GDP Active Directory domain controller located in the ABC corporate TCP/IP network is required – no GDP AD domain controllers will be installed within the VPN DMZs. The network latency incurred as a consequence of this "lookup" will need to be further investigated, however, from a server platform perspective, the ABC type seven server that is specified for the role of hosting the IAS service is comfortably within its performance parameters.

The sizing of any SecurID infrastructure servers is outside of the scope of this project.

APPENDIX A. SERVER CERTIFICATE SPECIFICATION

Template Display Name: **ABC ISA VPN Server**

This display name appears in the properties of issued certificate and makes ownership and purpose clear and unambiguous.

Minimum Key Size: **1024 Bit**

The key size dictates the strength of the RSA public / private key pair. A selection of 1024 bit is standard best practice for server authentication certificates.

Validity Period: **Two Years**

Specification of the certificate validity period is generally a trade-off between the expected assurance from certificate compromise arising from time-based brute force attacks and the administrative overhead of certificate renewal. The selection of two years provides a suitable level of re-assurance for a 1024 bit key length certificate, whilst not overburdening the certificate renewal process. Note: certificate renewal will need to be performed “manually” for server certificates.

Private Key Export: **Denied**

There is no valid reason to enable the export of the private key material and hence this option is disabled.

Subject Name: **“CN=FQDN”, e.g. CN=ISA1**

The subject name that is supplied in the certificate enrolment request will be based upon the server’s FQDN. Additionally, the certificate’s *subject alternative name* field will contain the same FQDN.

Issuance Requirements **CA Certificate Manager Approval**

Server certificate submission to the issuing CA server will result in the request being put into a pending state, the explicit approval of a user holding the CA certificate manager role (by means of AD security group membership) will be required for the certificate request to be accepted and a certificate issued.

Issuance Policy Extension **Medium Assurance**

The issuance policy will be referred to in the certificate practice statement indicating the level assurance undertaken in the issuance of the certificate.

Underlying Template **RAS and IAS Server**

The ABC ISA VPN Server certificate template will be created using a duplicate of the RAS and IAS Server template and making changes as indicated above.

APPENDIX B. CLIENT AUTHENTICATION CERTIFICATE SPECIFICATION

Template Display Name: **ABC Client Authentication**

This display name appears in the properties of issued certificate and makes ownership and purpose clear and unambiguous.

Minimum Key Size: **1024 Bit**

The key size dictates the strength of the RSA public / private key pair. A selection of 1024 bit is standard best practice for client authentication certificates.

Validity Period: **Two Years**

Specification of the certificate validity period is generally a trade-off between the expected assurance from certificate compromise arising from time-based brute force attacks and the administrative overhead of certificate renewal. The selection of two years provides a suitable level of re-assurance for a 1024 bit key length certificate, whilst not overburdening the certificate renewal process. Note: certificate renewal will be performed "automatically" using group policies.

Renewal Period **One Year**

The group policy auto-enrolment engine will attempt to renew the certificate one year prior to expiry.

Private Key Export: **Denied**

There is no valid reason to enable the export of the private key material and hence this option is disabled.

Subject Name: **Build from Active Directory**

The subject name format will specify the computer's FQDN and be "built from Active Directory". Additionally, the certificate's *subject alternative name* field will contain the FQDN.

Issuance Requirements **None**

Membership of the Active Directory "ABC VPN Computers" security group will entitle the computer to automatically enrol for a client certificate.

Issuance Policy Extension **Low Assurance**

The issuance policy will be referred to in the certificate practice statement indicating the level assurance undertaken in the issuance of the certificate.

Underlying Template **Workstation Authentication**

The ABC VPN Client certificate template will be created using a duplicate of the Workstation Authentication template and making changes as indicated above.

APPENDIX C. REMOTE ACCESS POLICY DETAIL

C.1 Policy Conditions

Authentication Type matches "EAP"

Client-Vendor matches "Microsoft"

Day-And-Time-Restrictions matches "Sun 00:00-24:00,Mon 00:00-24:00, etc"

NAS-IP-Address matches "x.x.x.x,y.y.y.y"

NAS-Port-Type matches "Virtual (VPN)"

Tunnel-Type matches "Layer Two Tunnelling Protocol (L2TP)"

Windows-Groups matches "corebus1.ABC.org\VPN Users"

C.2 Profile Settings

Idle-Timeout-Minutes = 60

Session-Timeout-Minutes = 240

EAP-Methods = RSA Security EAP

Encryption = Strongest

Framed-Protocol = PPP

Service-Type = Framed