Radiator
Digipass Support

This white paper discusses Radiator support for Vasco Digipass authentication tokens.

1.0 Introduction

This document shows how you can use Radiator, the full source Radius server from Open System Consultants (www.open.com.au/radiator) with Digipass authentication tokens from Vasco (www.vasco.com)

Radius is the de-facto standard protocol for authenticating users and for recording accounting information for dialup, wireless and wired LANs. See RFCs 2138, 2139, 2865 and 2866 for more details on the Radius protocol (www.ietf.org).

Vasco Digipass tokens are small handheld devices that generate one-time-passwords that change every 36 seconds. They can be purchased from Vasco and issued to your users. Such tokens provide much higher levels of security than static passwords that users have to remember. All Digipass tokens support two-factor authentication with per-user PINs. Some types of Digipass token can also operate in a Challenge-Response mode for yet higher levels of security. Vasco Digipass is supported by Radiator on Linux, Solaris, and Windows. Radiator supports the full range of Vasco Digipass software and hardware tokens on dialup, wired and wireless 802.1X capable LANs.

FIGURE 1. Some types of Vasco Digipass authentication tokens

GO-1 GO-3 Pro 300

Radiator is a highly configurable and extensible Radius server that allows you to easily customize and control how to authenticate users and record usage accounting information. Radiator works with a wide range of dialup, wired and wireless networking devices, ensuring that users satisfy security requirements before they can access the network. Radiator supports a wide range of authentication protocols, including Radius PAP, CHAP, MSCHAP, MSCHAPV2, SIP, EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-MSCHAPV2 etc.

Radiator supports a wide range of authentication methods, including Vasco Digipass tokens, SQL, LDAP, RAdmin and a range of ISP billing and user management systems. This extreme flexibility means that operators can use Digipass tokens for authentication on their own, or integrate Digipass authentication with new and existing custom and third-party user billing and management systems, for complete and secure user management in dialup, wired and wireless networking environments.

Radiator supports native Digipass authentication, where authentication is done directly by Radiator. It does not require the Vasco VACMAN Middleware software to authenticate tokens.

The combination of Radiator and RAdmin, the web-based user administration software from Open System Consultants allows operators to deploy a complete, easy-to-use web-based two-factor token administration and security system on Linux, Solaris and Windows platforms.

2.0 What are Digipass Tokens?

2.1 Overview

Digipass tokens are small, inexpensive hand-held devices that are issued to each end user that is to be permitted access to your network. When the user presses a button on the token, it shows a unique one-time-password (called a tokencode) on its display. The tokencode changes every 36 seconds by default and changes in an unpredictable way that is unique to each token.

Different types of token are available from Vasco in different formats and with different capabilities. Each token is supplied by Vasco with its own unique token data file. This token data file (called a DPX file) is imported by the administrator into the token database when the token is issued to a user.

Most Digipass tokens support user-assignable PINs (also called Static Passwords by Vasco) in order to provide two-factor authentication. Some types of Digipass token (e.g. Pro 300) require the user to enter their PIN into the token's keypad before the token will generate the tokencode. Other types without a keypad (e.g. GO-1 and GO-3) store the PIN in the Digipass database, and the PIN is combined with the current tokencode to generate the user's password. Some other types of Digipass support Challenge/Response, where the user has to enter a challenge code into the token before the tokencode will be generated. Radiator supports all types of Digipass token.

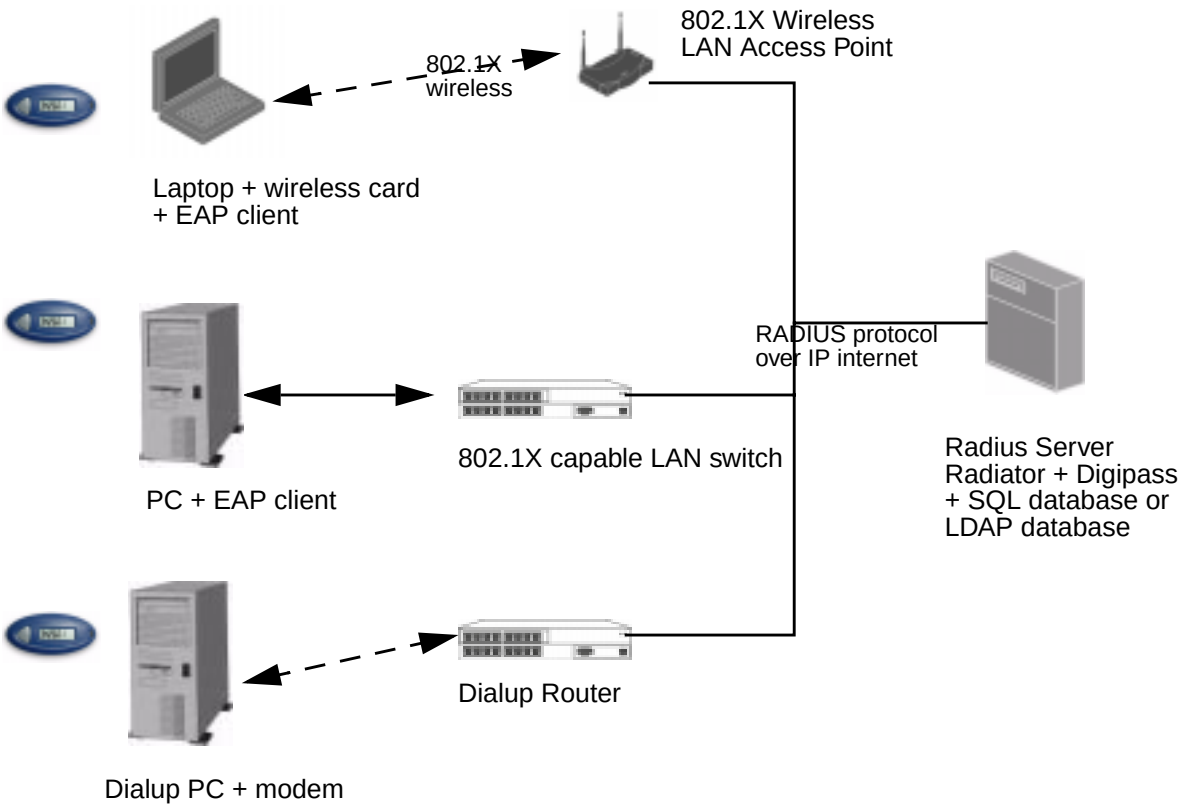
2.2 How Digipass authentication works

When a user wishes to connect to a dialup, wired or wireless network protected by Radiator and Digipass, they enter their username and as their password, they enter the current tokencode displayed on their token. If the token does not have a keypad, they prefix the tokencode with their current personal PIN.

The network access device (dialup router, wireless LAN access point, wired LAN switch etc.) sends the username and password to Radiator using the Radius protocol. Radiator finds the user and token details in its token database and then uses the integrated Vasco Controller to check the tokencode. If the tokencode is correct for that user, Radiator tells the network access device to permit the user to connect to the network. From that time, the user is connected to the network, and can use the network freely until they disconnect.

Most network access devices also send Accounting Start and Accounting Stop messages using the Radius protocol. Radiator can save this accounting information in an accounting database, for use by a separate user management program such as RAdmin. RAdmin can then use this data to display the login history for each user, or a list of users currently connected etc.

FIGURE 2. Typical elements of a Radiator Digipass authentication system



2.3 Security

Radiator and Digipass tokens together provide a higher level of security than ordinary static passwords that users have to remember and keep secure.

2.3.1 PINs

Most Digipass tokens support PINs (also called Static Passwords by Vasco) for increased security. The user must combine their secret PIN with the current tokencode before they can log in. This provides protection against an attacker finding or stealing the token. The requirement to have both the token and their personal secret PIN before they can authenticate is called ‘two-factor’ authentication. Support for PINs by a particular token requires that the token data issued by Vasco includes support for ‘Static Password’.

GO-1 and GO-3 tokens permit users to set and change their own PINs. The PIN is stored in the Radiator Digipass database, but users can change their PIN by using special combinations of tokencode, their old PIN and the new PIN.

Some types of Digipass token that include a keypad require the user to enter their PIN into the token before the token will generate the tokencode.

2.3.2 Challenge/Response

Some types of Digipass token also support Challenge/Response. In Challenge-Response, when you first attempt to log in, Radiator sends a 'Challenge' (a sequence of digits) that you must enter into the token in order to generate the correct Response, which is then used as your password.

2.3.3 Replay Attacks

Radiator and Digipass automatically protect against replay attacks. Any attempt to use the same correct tokencode twice in succession will result in the second attempt being rejected. This prevents eavesdroppers from using sniffed tokencodes to log in.

2.3.4 Configuration and customization

Radiator supports the customization of all the Digipass Controller run-time control parameters, including keys for storage of token data, maximum number of successive errors before lockout, maximum number of inactive days etc. This means that Digipass can be configured to suit the specific security needs of your organization.

3.0 Digipass support in Radiator

Radiator Radius server is developed in a modular way to permit easy configuration, extension and enhancement. It is delivered with support for a number of protocols, and a wide range of internal and external authentication methods and user databases. It can also be configured to authenticate from one or more local or remote databases, allowing multiple authentication systems to be combined and integrated.

Radiator suports Vasco Digipass tokens in SQL and LDAP databases and via the Vasco NMAS method for Novell eDirectory.

3.1 AuthBy SQLDIGIPASS, AuthBy LDAPDIGIPASS

Radiator's AuthBy SQLDIGIPASS or AuthBy LDAPDIGIPASS plug-in modules are used to authenticate Digipass tokens. AuthBy SQLDIGIPASS uses any free or commercial SQL database to find each user's token data. AuthBy LDAPDIGIPASS uses any free or commercial LDAP server to find each user's token data. These modules use the Authen-Digipass module, which is supplied with Radiator for Linux, Solaris, and Windows.

Radiator can be configured for use with Vasco Digipass in a variety of ways:

- As a simple stand-alone system. A single SQL table or set of LDAP records contains information about each Digipass token and the user it is assigned to. You can use the

digipass.pl command-line program supplied with Authen-Digipass to import tokens, assign them to users and otherwise administer tokens and users. The example digipass.cfg and digipass_ldap.cfg Radiator configuration files show simple examples of how to configure Radiator for such a system. Sample SQL database table definition files are provided with Radiator for a range of free and commercial SQL databases. Sample LDAP schema for use with OpenLDAP and otehr compatible LDAP servers are also supplied.

- As an addition to a Radiator-compatible user-management system or ISP billing system. In this mode, Radiator is configured to authenticate using AuthBy SQLDIGIPASS from an SQL table or AuthBy LDAPDIGIPASS from an LDAP server, but also uses other information from the user-management system to save usage data, get user- or service-specific Radius reply items etc.
- In conjunction with RAdmin Radius user management system from Open System Consultants (http://www.open.com.au/radmin). RAdmin provides an easy-to-install, easy-to-use web-based graphical system for managing Radius users for dialup, wired and wireless authentication. RAdmin version 1.9 includes support for importing, allocating and administering Digipass tokens for authenticating users against Digipass instead of static passwords. RAdmin also works with any free or commercial SQL database.

Radiator's extensive configurability and portability means operators can integrate Radiator and Digipass into almost any new or existing environment, providing high levels of security and usability.

Radiator supports Digipass authentication through Radius-PAP, Radius-CHAP, Radius-MSCHAP, Radius-MSCHAPV2, EAP-MSCHAPV2, PEAP-MSCHAPV2, EAP-TTLS-PAP, EAP-One-Time-Password or EAP-Tokencard protocols etc., which means that Radiator can authenticate access through almost any dialup router, or any 802.1X capable wired or wireless LAN device. Use of 802.1X EAP protocols generally requires the installation of appropriate EAP client software on the connecting PC.

Sample configuration files for a wide range of applications, including Digipass are included with Radiator for easy installation.

3.2 AuthBy LDAP2 with NMAS support

Novell eDirectory is a widely used user and identity management system based on LDAP (www.novell.com)

NMAS (Novell Modular Authentication System) is a component of eDirectory that permits eDirectory to authenticate passwords in a modular way. It allows third parties to add password authentication mechanisms (called Methods) to eDirectory.

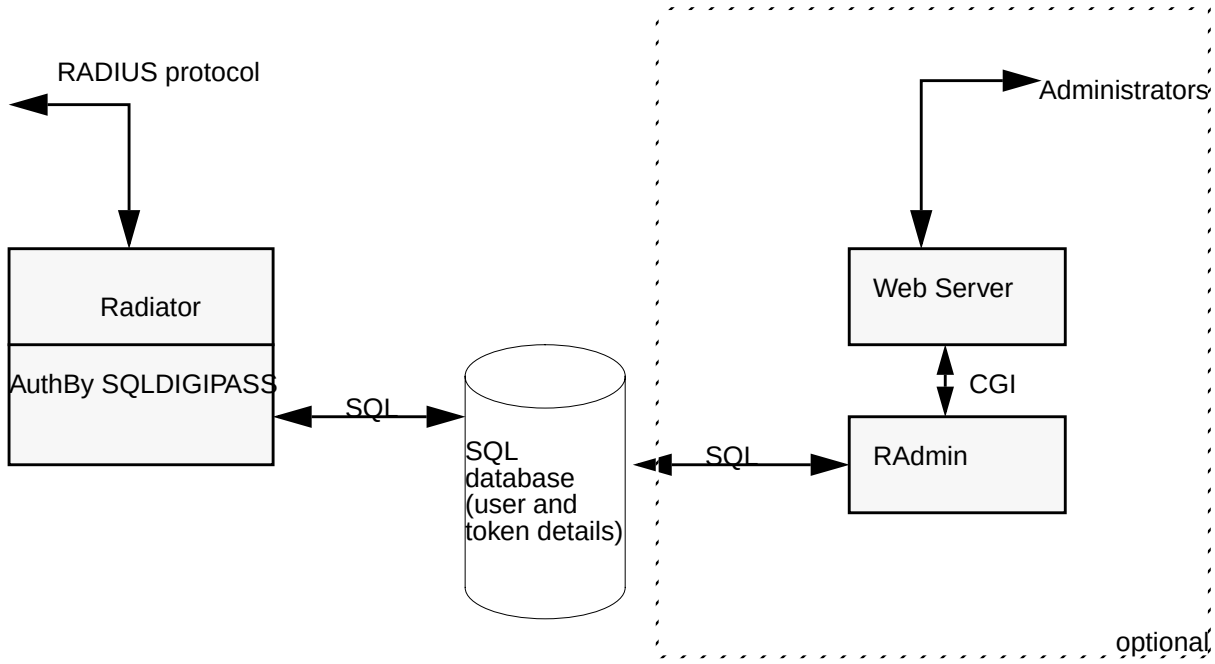
Vasco have released such an NMAS Method for their Digipass 2 factor tokens. This allows administrators to use eDirectory to import, manage, assign and authenticate Vasco Digipass tokens for their users.

Radiator now NMAS authentication of Vasco Digipass tokens (and other NMAS Methods). During NMAS authentication, PAP passwords are passed to eDirectory and the selected NMAS Login sequence method. The NMAS methods authenticate the password and tell Radiator whether to accept or reject the password.

Sample configuration files and Novell eDirectory NMAS installation hints are included.

4.0 Digipass support with RAdmin

FIGURE 3. Radiator + RAdmin Digipass architecture



RAdmin, the web-based Radius user management program from Open System Consultants (www.open.com.au/radmin) also supports Vasco Digipass tokens, and runs on a wide range of platforms.

RAdmin provides web pages that allow administrators to add, remove and change lists of users who are permitted to log in. RAdmin also allows administrators to drill down to detailed information about login history, users currently on-line, transaction logs etc.

RAdmin also optionally supports Digipass tokens. Administrators can import Vasco token data files (DPX files), and then assign or reassign tokens to users.

RAdmin works with Radiator and any free or commercial SQL database. The SQL database is used to store user, token and accounting data. Radiator then accesses the SQL database directly to authenticate users and tokens and to save accounting data.

The combination of Radiator and RAdmin results in a tightly integrated, high performance easy-to-use web-based user administration package that supports Digipass tokens for some or all users.

5.0 Migration

Along with Digipass, Radiator supports a number of other leading token-based authentication systems. In fact, Radiator can support several token-based authentication systems at the same time. This means that, when Radiator is installed, migration to Digipass from other token systems can be phased in gradually on a per-user or per-group basis, making migration to Digipass much easier than otherwise.

A common strategy when migrating from another token based authentication system to Digipass is first to install Radiator working with the existing token system, and then configure it to support both types of token, gradually migrating users to the user of Digipass tokens, and then to finally disable further use of the old token system.

6.0 Further information

Operators can choose to install and configure Radiator and Digipass support themselves, or Open System Consultants can provide assistance with installation, training, contract consulting and development. Contact info@open.com.au.

Open System Consultants can also put operators in contact with suitable prime contractors for deployment of a complete Radiator Vasco Digipass solution, including tokens, software, installation and commissioning. Contact info@open.com.au.

Various levels of pre-paid support are available from Open System Consultants, ranging from limited volume email support contracts through to 24x7 telephone support. Contact info@open.com.au for more details.

For pricing on Radiator and RAdmin products and support, contact info@open.com.au, or go to **http://www.open.com.au/ordering.html**.

With over 10 million current users of its DIGIPASS products, VASCO has established itself as a world leader for Strong Authentication with over 250 international financial institutions, approximately 1200 blue-chip corporations, and governments representing more than 60 countries.

To find more information about VASCO please visit **http://www.vasco.com** and click on '**where to buy**' to locate the nearest VASCO partner in your region.