



**DIGIPASS Plug-In for RACF**  
White Paper



# DIGIPASS Plug-In for RACF

## Whitepaper

---

<b>CONTENTS</b> .....	<b>2</b>
<b>OVERVIEW</b> .....	<b>3</b>
<b>PROBLEM DESCRIPTION</b> .....	<b>3</b>
<b>DIGIPASS PLUG-IN FOR RACF ON THE WEB</b> .....	<b>3</b>
<b>TECHNICAL CONCEPT</b> .....	<b>4</b>
GENERAL OVERVIEW .....	4
LOGON SEQUENCE .....	4
IDENTIFICATION PROCESS.....	5
<i>CARD Pseudo File</i> .....	5
<i>USER Pseudo File</i> .....	5
<i>SURROGATE Pseudo File</i> .....	5
DIGIPASS ADMINISTRATION.....	6
<b>SYSTEM REQUIREMENTS</b> .....	<b>7</b>
<b>SAMPLE OF USE</b> .....	<b>7</b>
<b>ABOUT VASCO</b> .....	<b>7</b>



## Overview

VASCO Data Security has a long history of delivering strong authentication and one-time password solutions through our DIGIPASS family.

The DIGIPASS Plug-In for RACF gives the ability to utilize the strength of the DIGIPASS family (One Time Password login as Time Based Response Only) into your existing environment. The RACF integration is meant to offer the best security level with an extremely low cost deployment.

VASCO has strong experience in mainframe security due to its large banking customer base and the DIGIPASS Plug-In for RACF is a perfect answer for security-focused companies. DIGIPASS Plug-In for RACF can secure your corporate authentication flow as well as the new and extensive connections that z/OS, OS/390 offers with the Unix System Services extensions.

LDAP, WebSphere can be implemented with the highest level of security thanks to DIGIPASS Plug-In for RACF.

## Problem Description

Static passwords are generally known throughout the security community as being non-secure and easy to compromise. The challenge is to introduce one time password technology into your existing system and applications to secure the sensitive information accessed via a corporate or remote user.

VASCO's solution is to add DIGIPASS strong user authentication into the regular RACF authentication system so that any access or application that relies on RACF will instantaneously get benefits of strong authentication.

The following pages present how DIGIPASS authentication is integrated into RACF and what the range of utilization of the DIGIPASS Plug-In for RACF is.

## DIGIPASS Plug-In for RACF on the web

VASCO has dedicated informations for DIGIPASS Plug-In for RACF on the following site:

<http://www.vasco.com/>

## Technical Concept

### General Overview

The DIGIPASS Plug-In for RACF approach is to use dynamic passwords, generated by a DIGIPASS device, on each authentication request from any client to the RACF secured Mainframe system.

Associated to RACF, The DIGIPASS Plug-In for RACF is a unique user point of control and covers mainframe resources as a whole (TSO, CICS, IMS, TPX, APPC, MQ series etc).

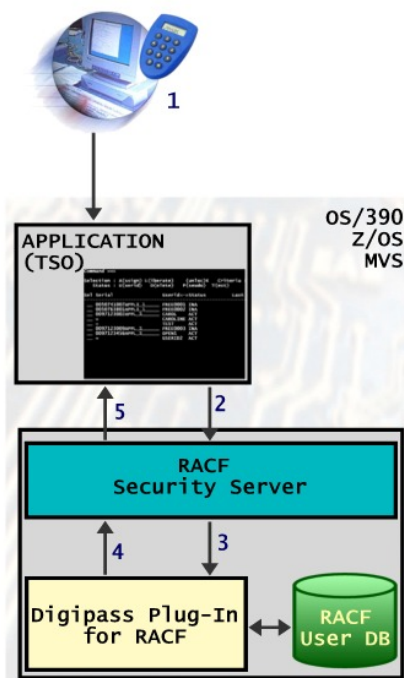
DIGIPASS data are (3DES) enciphered and then stored in the RACF database, providing an extreme confidentiality; RACF remains the identification control central point.

The DIGIPASS Plug-In for RACF is fully compatible with RRSF ensuring a robust platform as well as the easiest deployment.

The RACF database is at the same time classical passwords and DIGIPASS secrets holder ensuring authentication control and storage uniqueness (important factors for the access control system reliability in large environments).

### Logon sequence

RACF uses DIGIPASS Plug-In for RACF functions to validate the DIGIPASS dynamic authentication.



① A user logs on an application (TSO, CICS, IMS, TPX, APPC, etc) giving his UserID and his DIGIPASS dynamic password.

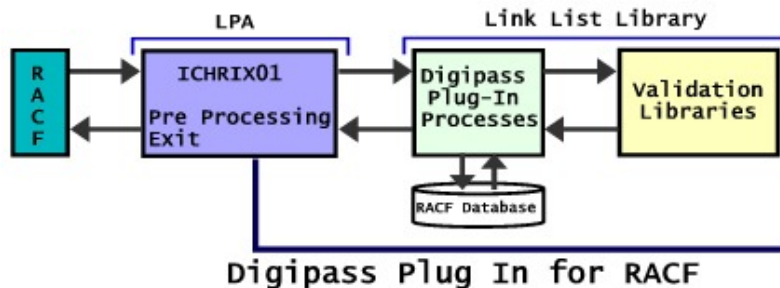
② The application forwards the authentication request to RACF with both UserID and Password.

③ RACF forwards this request to the DIGIPASS Plug-In for RACF.

④ The Digipass Plug-In for RACF accepts, rejects or indicates that it is not a DIGIPASS User. In this case RACF goes on the authentication on a classical way.

⑤ RACF accepts or rejects the access according to the received data from the DIGIPASS Plug-In for RACF and notifies the application.

## Identification Process



- RACF receives an authentication request from user U1 with password P1
- The RACF Exit ICHRIX01 intercepts this request and routes toward the DR2LRF01/DR2LRFDB
- DR2LRF01 reads in memory (ECSA) the CARD and USER pseudo files CLASS and PREFIX
- DR2LRFDB searches the user U1 relevant Data in RACF resource. If it one exists it extracts the user's status and its DIGIPASS serial number from the User's resource DATA field.
- If the user's status is ACTIVE, the DIGIPASS RACF resource (Prefix.Serial number) is retrieved to extract the DPDATA from the data field.
- A password-checking request is sent to the VACMAN Controller. Provided parameters are password P1 and the DIGIPASS DPDATA.
- The VACMAN Controller response follows program-call stack, up to RACF, that accepts or rejects the initial identification request.

## Data Storage

The DIGIPASS Plug-In for RACF uses the secure RACF database to store sensitive data. For its usage, the DIGIPASS Plug-In for RACF needs three 'pseudo files' that actually are database's entries but have all file related methods.

### CARD Pseudo File

This pseudo file contains DIGIPASS information such as secrets and operating mode; this data is triple DES encrypted.

### USER Pseudo File

This pseudo file contains USER related information and pointer to the DIGIPASS that have been assigned.

### SURROGATE Pseudo File

This pseudo file allows using multiple logon names (as the surrogate function allows) without being forced to assign several Digipass to a single physical user.

## DIGIPASS Administration

The DIGIPASS Plug-In for RACF comes with a complete administration interface that auto-extracts the parameters table from ECSA.

```
Digipass Plug-In for RACF - DIGIPASS Management -----
--
Command -->

You are going to assign the DIGIPASS n° 0050741007APPL1 1
To the User --> DUPONT      RACF Userid
Initial Status --> ACT      ACT/INA/PSW/CMD

If you answered CMD above, enter the desired status for each conditional
access path :

      --> ACT      --> ACT      --> ACT
      --> ACT      --> ACT      --> ACT
      --> ACT      --> ACT      --> ACT
      --> ACT      --> ACT      --> ACT
      --> ACT      --> ACT      --> ACT

PF3 Exit   Assign Digipass
```

*Digipass Administration Display Sample.*

It allows executing the following operations:

- Import Digipass file (DPX file)
- Add User
- Delete User
- User Status Change
- Assign Digipass
- Delete Digipass
- Unlock Digipass
- Test Digipass

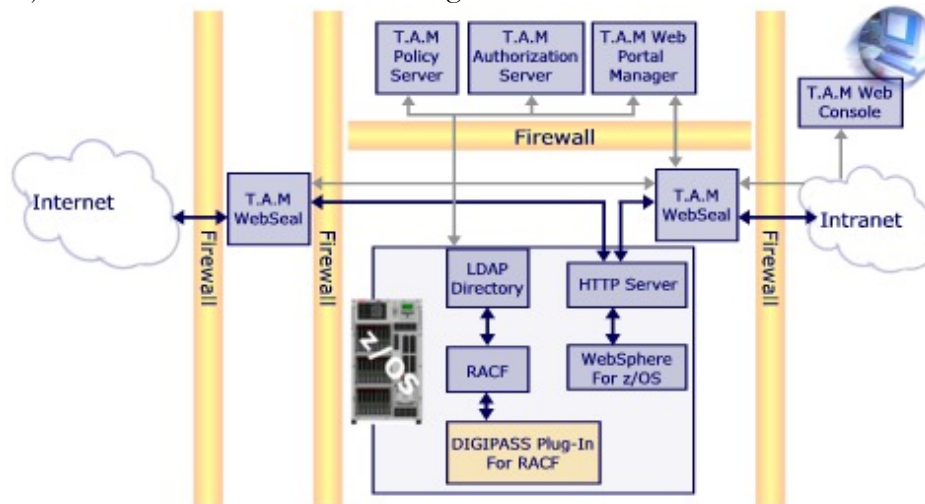
DIGIPASS Plug-In for RACF administration is performed through specific utilities grouped under an ISPF application; most of these utilities may also be run as batch programs to ease integration with existing administration tools.

## System Requirements

The DIGIPASS Plug-In for RACF can be installed on any z/OS or OS/390 that supports RACF.

## Sample of use

The following diagram shows a typical installation for a strong and complete DIGIPASS usage in conjunction with Tivoli Access Manager scheme.



## About VASCO

VASCO designs, develops, markets and supports patented “Identity Authentication” products for e-business and e-commerce. VASCO’s Identity Authentication software is carried by the end user on its DIGIPASS products that are small “calculator” hardware devices, or in a software format on mobile phones, other portable devices, and PCs.

At the server side, VASCO’s VACMAN products guarantee that only the designated DIGIPASS user gets access to the application.

VASCO’s target markets are the applications and their several hundred million users that use fixed passwords as security. VASCO’s time-based system generates a “one-time” password that changes with every use, and is virtually impossible to hack, or break. With 8 million current users of its DIGIPASS products, VASCO has established itself as a world-leader for strong Identity Authentication with 1300 international financial institutions, approximately 9000 blue-chip corporations, and governments representing more than 100 countries.