How-To Guide
Generate a Portal Public Key Certificate

Shows how to generate a Portal Public Key Certificate.

© Wolfgang Steinert
8/21/2008
# Table of Contents

Table of Contents ........................................................................................................... 2  
Synopsis .......................................................................................................................... 3  
Scope & Related Documents ......................................................................................... 4  
  Intended Audiences .................................................................................................... 4  
  Assumptions .............................................................................................................. 4  
  Scope exclusions ....................................................................................................... 4  
  Related Documents ................................................................................................... 4  
Implementation ............................................................................................................. 5  
Execution ....................................................................................................................... 6  
  Generating the Portal Public Key ............................................................................... 6  
  Using the Key ............................................................................................................ 8  
Appendix ....................................................................................................................... 9
## Synopsis

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>⚠️</td>
<td>Caution</td>
</tr>
<tr>
<td>🗣️</td>
<td>Example</td>
</tr>
<tr>
<td>💡</td>
<td>Note</td>
</tr>
<tr>
<td>🔧</td>
<td>Recommendation</td>
</tr>
<tr>
<td>👝</td>
<td>Syntax</td>
</tr>
</tbody>
</table>
Scope & Related Documents
This How-To document describes a procedure that is required to generate a SAP Enterprise Portal public key certificate that can be imported into an ECC client. This public key is used to verify SSO tickets presented to the ECC client in lieu of a user name and password for users to gain access.

The procedure takes into account common practices, SAP Best Practices, SAP requirements and Notes.

The purpose of this document is to document common procedures to simplify implementations of Portal requirements and to act as a source of reference for this and future implementations or developments

Intended Audiences
This document is intended for SAP BASIS administrators and related support groups. It does not provide assistance to inexperienced personal.

Assumptions
This document is based on the following assumptions:

• The user has administrative access to the instance.
• SSO between the SAP EP and R/3 is to be implemented
• The user is able to initiate operating system calls

Scope exclusions
This document does not cover all procedures required to implement SSO.

Related Documents
• How-To... Import a Portal Public Key into an ECC client.doc
**Implementation**

The SAP Portal public key certificate is required to enable single sign on using SAP logon tickets. The key is used to verify a logon ticket that is presented to an ECC client for logon in lieu of a user name and password a user normally has to provide.

The public key is generated by the portal, stored in a security certificate and imported into the SAP R/3 client by means of transaction STRUSTSSO2.

After a successful import the user may be signed on to the SAP client without the need to provide a user name and password, instead a signed SAP logon ticket is presented, verified against the public key and if valid the user is logged on.
**Execution**

To generate the portal key security certificate, the user must log in to the portal as administrator.

**Generating the Portal Public Key**

1. Log on to the portal as administrator

2. Navigate to “System Administration > System Configuration”


4. Select the TAB “Keystore Administration” from the Keystore Administration Window

5. Select the option “SAPLogonTicketKeypair-cert” from the drop-down menu

6. Click the button “Download verify.der File”
7. Click the “SAVE” button on the popup window

![File Download]

7. Click the “SAVE” button on the popup window

8. Specify the location where the file will be saved to. The file is a compressed .ZIP file with the default name “verify.der.zip”

![Save As]

8. Specify the location where the file will be saved to. The file is a compressed .ZIP file with the default name “verify.der.zip”

9. Save this file as verify.der.<SID>.zip substituting the <SID> with the actual SID.

You have now saved the public key in a certificate file for further distribution.

💡 To differentiate to which portal instance the certificate belongs it is advised to change the name of the certificate file to include the portal instance name (i.e. verify.der.C11.zip). This will allow for storing multiple certificates in one location and identify them by their SID.
Using the Key
To use the key in an SAP instance client please refer to the document “How-To... Import a Portal Public Key into an ECC client.doc”.