Startup process

Windows XP GINA logon

Soffid GINA is an optional part of Soffid ESSO. It's features are:

- Allows users to log on using smart cards. The digital certificates can be auto enrolled as long as there is a method to know which user it belongs to.
- Allows authorized users to log on with Local Administrator privileges.

Windows Vista Credential Provider

Soffid Credential Provider is an optional part of Soffid ESSO. It's features are:

- Allows users to log on using smart cards. The digital certificates can be auto enrolled as long as there is a method to know which user it belongs to.
- Allows authorized users to run with Local Administrator privileges.

Soffid session startup

After being identified by Windows, the Soffid session startup takes place. Either sequentially or in parallel to desktop startup, the Soffid ESSO session manager (named KojiKabuto after the best ever hero) is the responsible for making the following steps.

Update settings

KojiKabuto will contact Soffid servers o update registry entries using the system configuration introduced at Soffid console (LogonEntry, OfflineEntry, SSOServer, seycon.https.port)

Kerberos handshake

If it's enabled by system administrator, Soffid Synchronization server and the user desktop will perform a Kerberos handshake. If the Credential token shown by user desktop is accepted by any managed Active Directory, Soffid will accept that credential as a prove of identity.

In order to do that handshake, Soffid will create an special user named SEYCON_xxxx for each one of the synchronization servers involved in the login process.

Manual login

If it's enabled by system administrator, or Kerberos handshake has failed, the user will have the chance to enter it's user name and passwords. They will be verified by synchronization server against its internal user database.

Coordinates card

Once logged in, KojiKabuto requested permission to log. At this time, synchronization server could issue a coordinates card challenge. If the user fails to enter the right value for the coordinates requested, the Soffid session will be canceled.

Multiple sessions prevention

At this phase, Synchronization Server will check if the user has any other, not linked, session. If there is any other active session, and the user has not been granted the capability to open more than one (at Soffid console), the system will notice it to both, the new session and the ancient one.

Finally, the new session will take the decision to close the ancient one or to give up. If the user chooses to close the ancient one, the later will show a prompt, and its user will have 30 seconds to answer if he agrees to close that session. Usually the user has left the ancient session open and no user will be present at the ancient session. So, after 30 seconds the session will be closed and the new one will proceed.

SSO Rules activation

Once the session has been created, the SSO rules present at Soffid Console will be compiled and loaded into the Windows Session. Since this moment, every application launched will have its credentials automatically fullfilled.

Startup script

The workstation connects to Synchronization Server to get the session logon script (LogonEntry registry entry with deafault value "Logon"), and the session offline script (registry entry "OfflineEntry" with default value "offline"), which will be executed at next logon whether no Synchronization server is reachable.

The offline script is stored at %ProgramFiles%\SoffidESSO\Cache\offline.mzn file.

Afterwards, the application menu is populated using the application entries configured at Sofifd Console.

Desktop start

Unless the system configuration enables the user to use the desktop before opening the Soffid Sesion, the Desktop is started right now. Otherwise, the desktop would have been started at the

initial steps.

System operation

Once the session is started, Soffid ESSO has two main tasks to do:

> **First.** Timely keeps in touch with Synchronization server to confirm the validity of the soffid session.
>
> **Second**. Performs injection or user names and password to applications, based on the SSO rules bound to each application entry point the user is authorized to execute.\

Revision #1
Created 8 October 2024 14:44:46
Updated 8 October 2024 14:45:32