



eTrust SSO Fingerprint Authentication Agent (version 1.10)



A solution to meet the truly demanding needs of users, MIS professionals and security personnel.
A simple, tightly integrated Custom Authentication Scheme (CAS) for Computer Associate's eTrust platform that is secure, scalable and solution orientated from BIO-key™ International.

Strong user authentication and identification using biometrics is an essential addition to the eTrust SSO product. While the base eTrust SSO product provides robust single sign on authentication, it requires the use of a password that can be compromised. This integrated solution provides the ability for a user to login to a computer or computer network using eTrust SSO combined with unique fingerprint biometric identification without having to use a password, pin, card or token. Utilizing Vector Segment Technology (VST), our solution radically improves both the accuracy and speed of fingerprint-based recognition when compared to traditional methods.

Benefits include:

- Eliminating the overhead costs associated with password administration.
- Eliminating the vulnerability and exposure associated with a password being "hijacked" or compromised.
- Providing an easier to use solution for the user using a identification approach (1 to many search), not verification (1-to-1) which eliminates the need for a password, pin, card or token.
- Improved accuracy by certifying the identity of person at the computer with a fingerprint, relying on a human feature, (something you are) as compared to password or token based alternatives that rely on something you know (password) or something you have (token).

eTrust customers that use a Windows® SSO login can now protect their companies from fraud and streamline their current practices. The user is required to login only once; SSO then intercepts credential requests by specific applications and supplies the user's information for that application transparently.

Two extensions to the agent for the eTrust Single Sign-On system are available. The VST Fingerprint Client Extension enables fingerprint identification to log in and the VST Fingerprint Assistant Extension enables enrollment/deleting of a user's fingerprint record. In addition the VST Fingerprint Ticket Generator module enables communication between the agent and the SSO server and the VST Fingerprint Authentication Agent packages provide the availability of fingerprint identification for user authentication with the eTrust Single Sign-On system; the rest of the SSO system functionality and behavior remains unchanged.

Authentication Server:

The VST Authentication Server (VSTAS) provides the fundamental biometric services required for fingerprint authentication. The enrollment and authentication functions include:

- Storage of the VST model template
- Matching live a fingerprint template with a stored VST model template in a recognition (one to many matching) scheme
- Assigning an identifier, User ID (the Name on the SSO account) or VSTAS Operator ID, with each enrollment record
- Returning the User ID or Operator ID upon successful fingerprint recognition
- Storage of all data: - VST Model templates (one or all ten fingers) in cache and on disk, as required by the local SSO Security Administrator.
- The fingerprint agent uses the Microsoft SQL Server database as a central repository of the templates.

VST Fingerprint Ticket Generator:

A ticket is a block of data, secured through cryptography, containing the user's identification. The Fingerprint Ticket Generator acts as a "front-end" service to VSTAS in order to provide a ticket to the SSO Client when the user is logging in. The VST Fingerprint Ticket Generator functions in the following sequence:

1. Receives a request form the SSO Client containing the user's VST Model Template
2. Forwards the request to VSTAS, which returns a Name (User ID or Operator ID) upon successful recognition
3. Receives the Name (User ID or Operator ID)
4. Calls the SSO ticket validation process
5. Returns the newly generated ticket to the SSO Client

The ticket includes the user ID, BKFGFR as the Authentication Method being used, the VSTAS machine name, and a checksum calculated with the SSO Server key.

VST Fingerprint Assistant Extension Software:

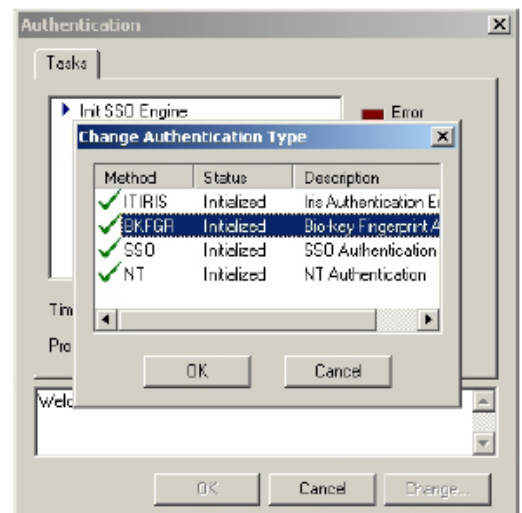
The VST Fingerprint Assistant Extension Software provides interactive administrative tools. Acting as administration clients, these tools allow a VSTAS Operator (usually a SSO Administrator) access to the server from a remote location. However, each

enrollment must be created at the SSO Assistant machine servicing a particular workstation. The Fingerprint Assistant Extension GUI presents and controls the process of user enrollment. This GUI is the primary interface, and is often the user's first experience with VST Fingerprint technology. There can be as many hosts with Fingerprint Assistant Extension software as the eTrust Single Sign-On network requires.

The following are the set of screens where the user can be enrolled, deleted, given access and set the configuration for the fingerprint method (BKFGFR) using the eTrust SSO Assistant:

VST Fingerprint Client Extension Software:

The VST Fingerprint Client Extension Software allows a workstation user to log into and use the services that the SSO system provides with Fingerprint authentication. The extension communicates VST Model Templates to VSTAS through the Fingerprint Ticket Generator port and accepts the return of an authenticated ticket. The extension may be configured to request fingerprint authentication as the primary login method.



For more information on BIO-key and our suite of products, call 800-400-6311

Copyright 2005, BIO-key International, Inc. All rights reserved. Product specifications are subject to change without notice. All BIO-key International, Inc. product names and logos are trademarks and/or registered trademarks. All other brands, product names, and company names mentioned here in may be trademarks or registered trade marks of their respective holders.

BIO-KEY INTERNATIONAL, INC.
CORPORATE HEADQUARTERS
3349 HIGHWAY 138
BUILDING D • SUITE A
WALL, NEW JERSEY 07719
WWW.BIO-KEY.COM