



S W U R V
s m a r t e e s

application architecture



Smartees allow Swurv Users to identify themselves to 3rd party applications without any User action or intervention. This allows a 3rd party application (*examples: e-tail, informational, ERP*) to request from Swurv the 3rd-party-specific identity of the User attempting a connection and, once connected to request further information about the User if it is required. The Swurv User always has the final decision on whether to grant or deny these permissions.

This single sign-on authentication occurs using secure data transmission protocols and keeps the User's Swurv Sign-on credentials secret from the 3rd party.



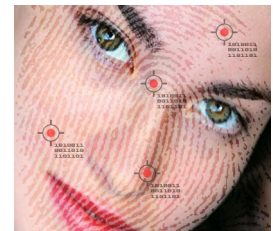
Connecting people to all of their relevant systems, enabling secure collaboration, and true, end to end transactions.



E-tailing: the selling of retail goods on the Internet. Short for "electronic retailing," and used in Internet discussions as early as 1995, the term seems an almost inevitable addition to e-mail, e-business, and e-commerce. E-tailing is synonymous with business-to-consumer (B2C) transaction.

The **Swurv Smartees Application Architecture** is designed to be democratic, distributed and organic in nature.

One of the most powerful characteristics of the Internet is its distributed and chaotic structure. It allows multiple pathways to the same point of data or communication, making its infrastructure both accessible and resistant to attack.



s m a r t e e s

Swurv User

A User currently signed on to the Swurv Environment.

Smartees

A unique item of information incorporating identification and permission exchanged between services in the Smartees Protocol.

Smartees Protocol

A sequence of calls to web services that provide secure interoperability between disparate applications.

3rd-Party Application

An application or Webservice provided by a 3rd-party that requires User authentication, User data or to participate in Smartee enabled business processes. This application is separate and distinct from Swurv PolyNet but is capable of using the Smartees protocol.

3rd-Party Specific User Information

Information about a User that is stored long term by Swurv for the 3rd-party application. This information is not available to other 3rd-party applications without owners permission. Examples include a customer number, access credentials or privileges.

3rd-Party Identity

Depending on the needs of the 3rd-party application it may be sufficient to know that the User attempting to connect to it is a Swurv User. This would be the case, for example, if the 3rd-party application will only need to know the User's mailing address at some point. The address would be queried from Swurv.

In other cases it may be necessary to determine specifically the 3rd-party identity (the credentials, rights and privileges of that User with respect to the 3rd-party application.) This information is stored as part of the 3rd-party specific User information. The User does not need to participate in the exchange-of or granting-of access to the 3rd-party identity.

Non-repudiation

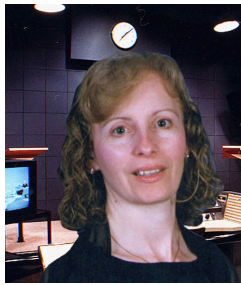
Non-repudiation is a property achieved through cryptographic methods which prevents an individual or entity from denying having performed a particular action related to data (*such as mechanisms for non-rejection of authority (origin); for proof of obligation, intent, or commitment; or for proof of ownership*).

Generic User Information

User information stored by Swurv that is available to all 3rd party applications. If the information is considered confidential to the User then Swurv will request permission from the User before granting access to the 3rd party application. Examples include the User's name and address.



An e-tailing Example Usage Scenario:



Meet Karen, a nutritionist, and Swurv User. She browses to a secured access B2B e-commerce website which understands the Smartee protocol.

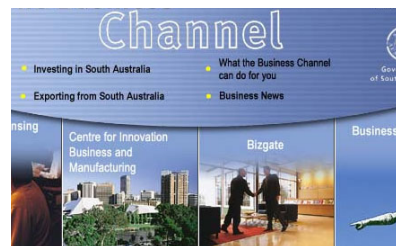
Before the website shows her a User name & password login screen, it first asks Swurv whether she is currently signed on through the Swurv Environment (SE).



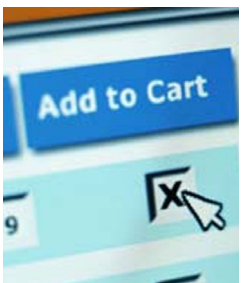
Karen browses the Internet to a secured access B2B e-commerce website which understands the Smartee protocol.



Once confirmed that she is signed on through SE, the website then asks Swurv for Karen's access credentials, automatically logging her into the website, bypassing the login page. If Karen was not using Swurv or did not have the credentials, the website would show her the normal login screen. This website is participating in a single sign-on system enabled by Swurv Smartees.



Since she is signed on through the Swurv Environment (SE), she is automatically logged in to the site.



Now Karen places a product in a shopping cart and heads to the checkout page. The website first asks Swurv for Karen's address so that it can pre-fill the delivery form. Since Karen's address is private information, Swurv first asks Karen whether the

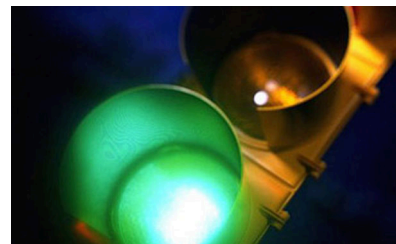
3rd party website may be granted permission to see her address.



When Karen makes a purchase on the website, she simply grants permission to her delivery address information.

Upon confirmation Swurv responds to the website with the address information which is shown pre-filled in the delivery form.

The advantage to the 3rd party application of requesting the address from Swurv is that if the address changes then the User only needs to update their address once, within Swurv, rather than in all of the other applications or Webservices they might also use.



The purchase is completed, and the delivery form is automatically filled in. If Karen changes her address, the e-commerce website has direct access to the updated information for as long as Karen grants them permission.

This single, distributed repository for User data along with Swurv access controls provides both the User and the 3rd party application with significant benefits.



Process Overview:

1. The User connects-to and Signs-on-to the Swurv Environment. (*Authentication*)
2. The User attempts to connect to a 3rd party application/Webservice. (*Example: an extranet website*)
3. The 3rd party application queries Swurv whether the User is a Swurv User. The 3rd party application creates a unique, encrypted temporary key that it passes to Swurv for further communications regarding this User.
4. Swurv registers the temporary key with the User's Swurv session and responds to the 3rd party application confirming that the specific User (*identified by the temporary key*) is a Swurv User.
5. The 3rd party application may now request from Swurv further information about the User. This information may be unique to the 3rd party application (*such as their customer number or access privileges*) or generic to the User (*such as their address.*)

Some of the Benefits of Smartees:

Returning User Identification/Authentication

Smartees solve the problems with permanent browser cookies such as the limited data storage potential, multiple User access devices, multiple User access browsers, different Users on the same browser, software or operating system reinstalls and cookie cleaning/sweeping applications.

User Privacy

The User has the right to decide what personal information to share with which 3rd party applications and can actively participate in the granting or refusal of access to requested information.

User Data Repository

The User maintains information in one location while retaining the right to govern access permissions to 3rd-party applications.

Central 3rd Party Data Repository

Long term storage of 3rd-party application information on a particular authentication server, allows the enabling of User identification and credential storage.

Proprietary Information Retention

Smartees do not require the disclosure of 3rd party application proprietary information to Swurv or other 3rd-parties.

Single Sign-On

3rd-party applications may receive User credentials without inconveniencing the User.

Complex Business Relationship and process interoperability

Smartees allow multiple 3rd party applications and Webservices to exchange information and take part in multi-step business processes while retaining security and individual application data confidentiality along with transaction non-repudiation.

Transmission Security and Authorization

The Smartee protocol takes advantage of generally known and available best-of-breed data exchange security and participant authorization protocols.

Application Level Programming Interface

Using generally known and available protocols allows 3rd-party applications to be developed using a wide variety of technologies without restrictions to particular operating systems or programming support layers.

Smartee is an Acronym for:

Smart Electronic **E**ncryption **S**equence

For Further Information:

Sales: sales@swurv.net

Technical: tech@swurv.net