



SECURE ENTRY SERVER YOUR SECURITY INFRASTRUCTURE

The Secure Entry Server by United Security Providers protects web applications in the internet and intranet and lowers operational costs. As a managed service it ensures compliance with legal liabilities concerning full retraceability of business transactions and offers convenient web Single Sign-On.

AVAILABILITY.

The architecture of the Secure Entry Server has been designed to be both highly available and scalable. The concept aims at integrating with existing high-availability solutions of established key players, at system-, network- and application-layer.

CONFIDENTIALITY.

The Secure Entry Server complements the firewall infrastructure with a central component for secure identification of users (authentication) as well as selective unlocking of applications (authorization). This ensures that any unauthorized access to application servers is prevented.

LOWERED OPERATIONAL COSTS.

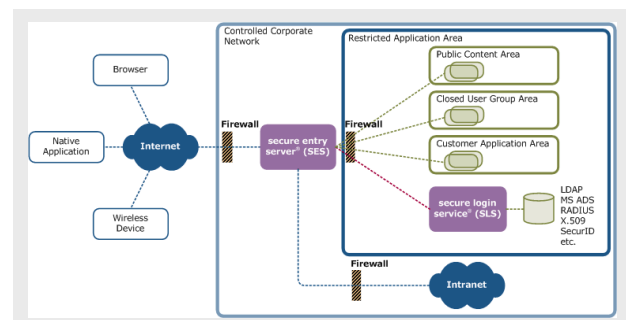
Thanks to the key position of the Secure Entry Server (SES) it is possible to integrate all or just individual groups of SES-protected applications into a Single-Sign-On network. As a result, the user has to log on to the Secure Login Service only once and is then given access to all authorized applications automatically. This functionality can be applied not only to custom, self-written applications but also to standard applications. All these functions allow for standardization and drastic reduction of the DMZ environment in terms of size. The outcome of this is significantly lower costs in respect of operation and maintenance. This check is done by the Secure Login Service which is physically separated from the SES for security reasons.

INTEGRITY.

The Secure Entry Server prevents direct connections between a lower classified network (such as the Internet) and a higher classified network (like a server network). It interrupts the session, removes any security-critical elements (headers, control blocks etc.) and creates a completely new session with the actual target destination. This already invalidates a large number of popular attack methods in principal, resulting in a highly increased access protection for the server environment.

RESPONSIBILITY OF MANAGEMENT.

Another challenge is to ensure that all the applications which are part of the core business comply with all legal liabilities coming into force more and more these days. Due to the rapid growth of applications over the last years, many companies fail to ensure the possibility to completely retrace business transactions. The Secure Entry Server as a single, central point of entry allows for chronological enquiry of all user activities. Furthermore, it facilitates the selective recording of workflow steps, without requiring the involved applications to support this explicitly.



Function architecture of Secure Entry Server.

SECURITY.

The Secure Entry Server protects itself and applications on both the network- and the application layer.

- Multiple, overlapping barriers against anonymous and authenticated attackers
- Session/Cookie-Store protects the applications against attacks on the session and allows cookie-free access for the client, even if the applications are using cookies.
- Protection against cookie stealing through SSL session ID (exceptions can be defined to support external viewers such as Media Player etc.)
- Protection against SQL-, scripting- (XSS) and other injection attacks.
- Central authentication (Single Sign-On) and user administration for varying application servers and different user databases.
- SSL/TLS for client- and server-connections with full, including server-side, session caching.



- Supports several crypto-accelerators.
- Secure administration access.
- Multi-compartment architecture based on certified operating system (Pitbull™).
- System minimizes risk of attacks.
- HTTP protocol filtering and protocol breach.

SCALABILITY, PERFORMANCE AND AVAILABILITY.

The Secure Entry Server minimizes the negative performance impact inherent to reverse proxy servers.

- Supports load balancing and fail-over (dynamic routing through SES, «SMP scaling» and «parallel server clustering»).
- Persistent end-to-end HTTP connections and SSL session resume minimizes response times and system resource usage.
- Configuration changes can be performed with absolutely no service outage or lost sessions.

RECORDING.

The Secure Entry Server supports Non-Repudiation.

- The recording subsystem logs user activities and allows for a later reconstruction of the complete communication with the application servers.
- Specific user data can be excluded from the recording.

Data can be viewed comfortably with any standard web browser.

UNIVERSAL, TRANSPARENT.

The Secure Entry Server integrates existing applications without changes.

- The Adaptive Application Integrator (AAI) provides extensive integration functionality.
- In a Single Sign-On system, several sessions can be combined into one single session.
- AAI allows to integrate applications which only support «Form Based Authentication».
- Other means of integration: X.509 certificate, «Basic Authentication» and HTTP headers.
- Can perform URL path translations; absolute URLs can be replaced.
- Dynamic routing. The Secure Login Service can designate target servers dynamically per user.

ADMINISTRATION, MONITORING.

The Administration is based on the standards set by the widely-used Apache Web Server.

- Widespread Apache know-how can be used.
- A large selection of administration- and security-tools is available.
- Secure, role-based administration.
- SSH included in standard delivery.

AUTHENTICATION.

The Secure Entry Server allows for one single authentication service to be used for all applications.

Authentication methods supported by the SLS:

- Username / password
- SecurID, strike-number, X.509 certificates
- LDAP (Microsoft ADS, Novell NDS, Netscape Directory)
- RACF
- RADIUS

OPEN, STANDARDIZED, EXTENSIBLE.

The Secure Entry Server is based on extensible Open Source components and committed to open standards.

- The SES is designed modular and can be extended based on customer requirements.
- Integration without change of applications: Certain security architectures do not required changes in applications, but plug-ins (filters) in application servers.

Based on the Apache™ Web Server and mod_ssl, existing modules can be used.