

AuthAgent Kerberos

Embedded Kerberos V Authentication



AuthAgent Kerberos is an embedded implementation of the Kerberos V authentication protocol (RFC 4120) for client agents and network services running on embedded platforms. Being fully interoperable with Unix® Kerberos Key Distribution Centers (KDCs) and Microsoft® Active Directory Services in Windows® servers, it allows for seamless secure authentication in heterogeneous environments. With Kerberos becoming a preferred authentication mechanism for several network security protocols and a required part of several industry specifications, **AuthAgent Kerberos** provides a convenient way to add highly-secure authentication to embedded devices.

AuthAgent Kerberos implements the protocol in RFC 4120 that specifies an authentication and encryption scheme that allows a principal to become "known" by an authenticating server and then to use that authentication to access systems and services on the network.

AuthAgent Kerberos provides the "magic

sauce" required for network client software as well as network services running on embedded devices to easily be Kerberos-enabled ("kerberized") and communicate with centralized Kerberos Key Distribution Centers (KDCs) which store user and service authentication databases. This allows an organization to leverage its enterprise network Kerberos servers to authenticate services and clients running on embedded devices such as networking and storage equipment, connected smart appliances, and remotely managed industrial control applications.

AuthAgent Kerberos also provides GSS-API support for use as a generic mechanism for authentication in other security protocols and ticket caching functionality. It has been validated against KDCs in UNIX, Linux and Windows server environments, including Windows Active Directory Services and secure domain authentication.

AuthAgent Kerberos has been extensively validated on a variety of CPU architectures, which minimizes development and integration efforts. The

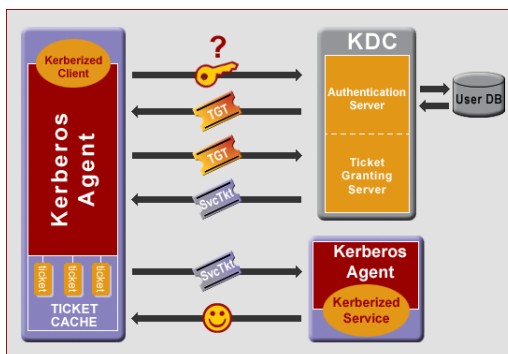


Fig 1: AuthAgent Kerberos Operation

Special Features

- ❖ Includes caching functionality
- ❖ Kerberos-enables (Kerberizes) both - network clients and services
- ❖ Enhanced memory management & partition support
- ❖ Multi-tasking support

Features

- ❖ Support for Kerberos V authentication.
- ❖ Kerberos-enables network clients and services.
- ❖ Allows single-logon convenience.
- ❖ Provides for integrity and confidentiality of encrypted Kerberos messages.
- ❖ Generates session key for authentication that may be used by application for session privacy.
- ❖ Replay protection.
- ❖ Ticket caching functionality.
- ❖ Interoperable with Kerberos KDCs, services and clients on other platforms.
- ❖ Validated against Microsoft Windows® Active Directory, Windows® Server and Linux®/UNIX® implementations.
- ❖ Proven interoperable implementation of PKINIT.
- ❖ IPv6 support.
- ❖ Can be used as a stand-alone module or add-on to network security solutions such as SSH and IPsec.
- ❖ Support for PowerPC, MIPS, X86, ARM/XScale CPUs.

AuthAgent Kerberos distribution includes sample kerberized clients and services (native mode and GSS API based) to use as reference implementations.

With Kerberos becoming a preferred authentication mechanism for several network security protocols and a required part of several industry specifications, **AuthAgent Kerberos** provides a convenient way to add highly-secure authentication to embedded devices outside the enterprise as well.

Secure Authentication

Transmission of plain-text authentication information such as passwords is clearly the weakest link in user authentication systems. It is susceptible to "eavesdropping" where the password itself is compromised, or "replay attacks" that simply retransmit previously sniffed encoded passwords to gain access to critical network services. The Kerberos protocol was specifically designed to eliminate the need to demonstrate possession of private or secret information (the password) by divulging the information itself. Additionally, **AuthAgent Kerberos** includes data integrity checks to ensure that messages on the network are not tampered with, and message privacy.

Tickets and Key Distribution

The basic unit that a Kerberos system uses to avoid sending passwords in the clear is called a "ticket". A Kerberos ticket is a record that allows a client to authenticate itself to a service. It contains the client's identity, a session key, a timestamp, and other information, all sealed using the service's secret key. Kerberos tickets are given out by an enterprise network service called the Key Distribution Center (KDC), which supplies tickets and temporary session keys, and hosts a database of users and services. **AuthAgent Kerberos** provides the functionality for embedded network clients present and store KDC granted tickets to any Kerberos-enabled network services. It also includes the functionality to present the initial Ticket Granting Ticket Granting Service (TGS) for service-specific tickets.

PKINIT

AuthAgent Kerberos can perform the initial authentication using X.509 formatted digital certificates as described in RFC 4556 (Public Key Cryptography for Initial Authentication in Kerberos – PKINIT). **AuthAgent Kerberos'** PKINIT implementation is interoperable Heimdal and Windows

Active Directory implementations when used in combination with **TeamF1's AuthAgent X.509** product. **AuthAgent X.509** accepts certificates as files or as smartcard. Smartcard support is implemented using PKCS11.

Single Logon

When the principals being authenticated are users, **AuthAgent Kerberos** enables a single sign-on solution. Clients have to authenticate themselves only once to the KDC to obtain an initial TGT ticket. Further service specific tickets are automatically granted via a ticket-granting service (TGS) during validity of the TGT. **AuthAgent Kerberos** allows for caching the individual tickets allowing them to be re-used until their validity expires, eliminating the need to repeatedly request tickets for the same service.

Kerberos-enabled Clients & Services

AuthAgent Kerberos easily "kerberizes" embedded clients, allowing standard network client applications in any multi-platform environment to authenticate to Kerberos-enabled services. Similarly, network services that need to be Kerberos-enabled, and accept ticket-based authenticated sessions, can be secured with **AuthAgent Kerberos**. Kerberos-enabling of embedded clients and services is achieved using very few simple API calls during session initiation or initialization respectively.

Standards-based Encryption

AuthAgent Kerberos includes support for the latest standards-based ciphers for data encryption and message integrity verification, such as:

- ❖ Triple-DES/DES
- ❖ AES
- ❖ SHA-1
- ❖ MD-5
- ❖ CRC

Applications

AuthAgent Kerberos may be used in application-level protocols, such as

Also Available

- ❖ **AuthAgent RADIUS**
RADIUS Authentication Agent
- ❖ **AuthAgent X.509**
Digital Certificate Authentication
- ❖ **SSHield**
Secure Shell & SFTP/SCP
- ❖ **V-IPSecure IPsec & IKE**
Network Layer Security

Customization Flexibility

All **AuthAgent** solutions are available in full-source format and are highly customizable. **AuthAgent Kerberos** has configurable options for user-specific credential caching as well as user-specific ticket restrictions. Complete scalability of unwanted components makes **AuthAgent** solutions the solution of choice for embedded security applications.

RFC Support

- ❖ RFC 4120
- ❖ RFC 2743
- ❖ RFC 3962
- ❖ RFC 1964
- ❖ RFC 2744
- ❖ RFC 4121
- ❖ RFC 4556

telnet or FTP, to provide "user to embedded device" security or as the implicit authentication system of data streams or RPC mechanisms. It can also be used at a lower level for "embedded device to host security" or between embedded devices, in any standard or proprietary network protocols including IP, UDP, and TCP. It also finds application in larger credential based frameworks such as GSS-API. **AuthAgent Kerberos** is designed to be used as a standalone authentication mechanism in applications where only access control is important, or as a seamless add-on to network security solutions such as **TeamF1's SSHield SecureShell** and **V-IPSecure IPsec/IKE**, where its authentication can be used along with network security protocols that protect data in transit.

Email: sales@TeamF1.com
Web: www.TeamF1.com
Ph: 510-505-9931 ext. 5
Fax: (510) 505-9941



© 2002-2007 TeamF1, Inc.