

Devicescape Agent

For Secure and Easy to Use Wireless Devices



Powered by the Devicescape Agent
RIM BlackBerry Bold



Powered by the Devicescape Agent
Sharp LCD Monitor

Device makers worldwide are looking to leverage the tremendous proliferation of Wi-Fi networks and incorporate the convenience of wireless connectivity into every type of device imaginable, from home entertainment electronics to portable handsets to office automation equipment. The Devicescape Agent provides device manufacturers with a robust software solution for creating a broad range of devices that can wirelessly connect to the Internet, as well as other wireless devices. Typically running in the user or application space of a device's operating system, the Devicescape Agent handles the setup, management and termination of secure Wi-Fi connections. The Devicescape Agent is suitable for OEM and ODM embedded devices, PC OEM applications, and semiconductor reference designs. The Devicescape Agent offers complete support for WPA2 security, Cisco Compatible Extensions (CCX), and the Wi-Fi Protected Setup specification that enables devices to be automatically configured with the push of a button. Additionally, the Devicescape Agent is designed to easily integrate with the Devicescape Connect solution, enabling devices to seamlessly connect to Wi-Fi hotspots.

Comprehensive Security

The Devicescape Agent supports the entire suite of Wi-Fi security mechanisms that are currently used in practice, including WEP, dynamic WEP with 802.1X, WPA/WPA2 Pre-Shared Key, and WPA/WPA2 Enterprise. A full range of 802.1X Extensible Authentication Protocol (EAP) methods are provided to enable deployment in any type of enterprise security environment (see the technical specifications on the back page for a complete list of supported EAP methods). It is straightforward for developers to remove code for unnecessary EAP methods, or add new EAP

methods. The Devicescape Agent can store multiple network definitions (or preference lists) in order to quickly reconfigure itself for various wireless networks. The software also supports 802.11i RSN roaming via pre-authentication. For EAP methods utilizing certificates (e.g., EAP-TLS, EAP-TTLS, PEAP and EAP-FAST), the Devicescape Agent supports an interface to external SSL/TLS libraries for certificate processing. The open source OpenSSL library is included in the product, and the Devicescape Agent has also been deployed with small footprint commercial SSL/TLS libraries from Certicom and PeerSec Networks. The Devicescape Agent has been tested to interoperate with the popular RADIUS authentication servers from Cisco Systems, Funk, Meetinghouse and Microsoft.

Wi-Fi Protected Setup

Devicescape's implementation of the Wi-Fi Alliance's Wi-Fi Protected Setup specification makes it easy for consumers to configure and use a wireless network. The Devicescape WPS solution has been tested using a super-set of the Wi-Fi alliance test plan, and verified for interoperability against a large number of commercial access points. This ensures seamless compatibility and avoids some of the pit falls with early WPS implementations. The Devicescape Agent supports automated configuration of wireless security and network settings via both the PIN code method and the convenient Pushbutton method. A device can act as an Enrollee, or as a Registrar for setting up an unconfigured access point. When included in a device's firmware build, Devicescape's implementation of Wi-Fi Protected Setup adds only about 70 KB to the memory footprint. Devicescape can also provide a Wi-Fi Protected Setup-compatible router for interoperability testing purposes.

Benefits to Device Companies:

With the proven Devicescape Agent, device manufacturers can realize the following benefits:

- Accelerated time to market and lowered development costs with complete, mature and validated wireless software technology
- Assurance of Wi-Fi certification and interoperability with full IEEE 802.11 and Wi-Fi Alliance standards support
- Interoperability with the Cisco enterprise wireless LAN infrastructure via complete CCX support
- Flexibility in device design with broad Wi-Fi chipset, processor and OS support
- Lower post-sales costs and improved end-user satisfaction with Wi-Fi Protected Setup
- Optimized for integrating the award-winning Devicescape Connect or Devicescape Connect Service solution

Wi-Fi Certification Assurance

The Devicescape Agent's Wi-Fi technology is pre-certified against the IEEE 802.11 standards and the Wi-Fi Alliance specifications. In fact, Devicescape's WPA, WPA2 and Extended EAP mode implementations are employed as the golden reference standards in the Wi-Fi Alliance's certification test bed. Device manufacturers can thus have confidence that their Devicescape-based products will be interoperable and achieve Wi-Fi certification in a timely manner.

Cisco Compatible Extensions

In order to ensure interoperability with the large installed base of networking infrastructure equipment from Cisco Systems, the Devicescape Agent supports Cisco Compatible Extensions as an option. The CCX option provides support for up to version 5 of the CCX specifications (in conjunction with selected operating system platforms and Wi-Fi chipset drivers), and includes features such as enhanced EAP-FAST, CCKM, CKIP, and Cisco roaming and voice features. Wireless devices using the Devicescape Agent with CCX can take advantage of Cisco's innovations for enhanced security, mobility, quality of service, and network management as an option for Cisco CCX Program Licensees.

Devicescape Connect

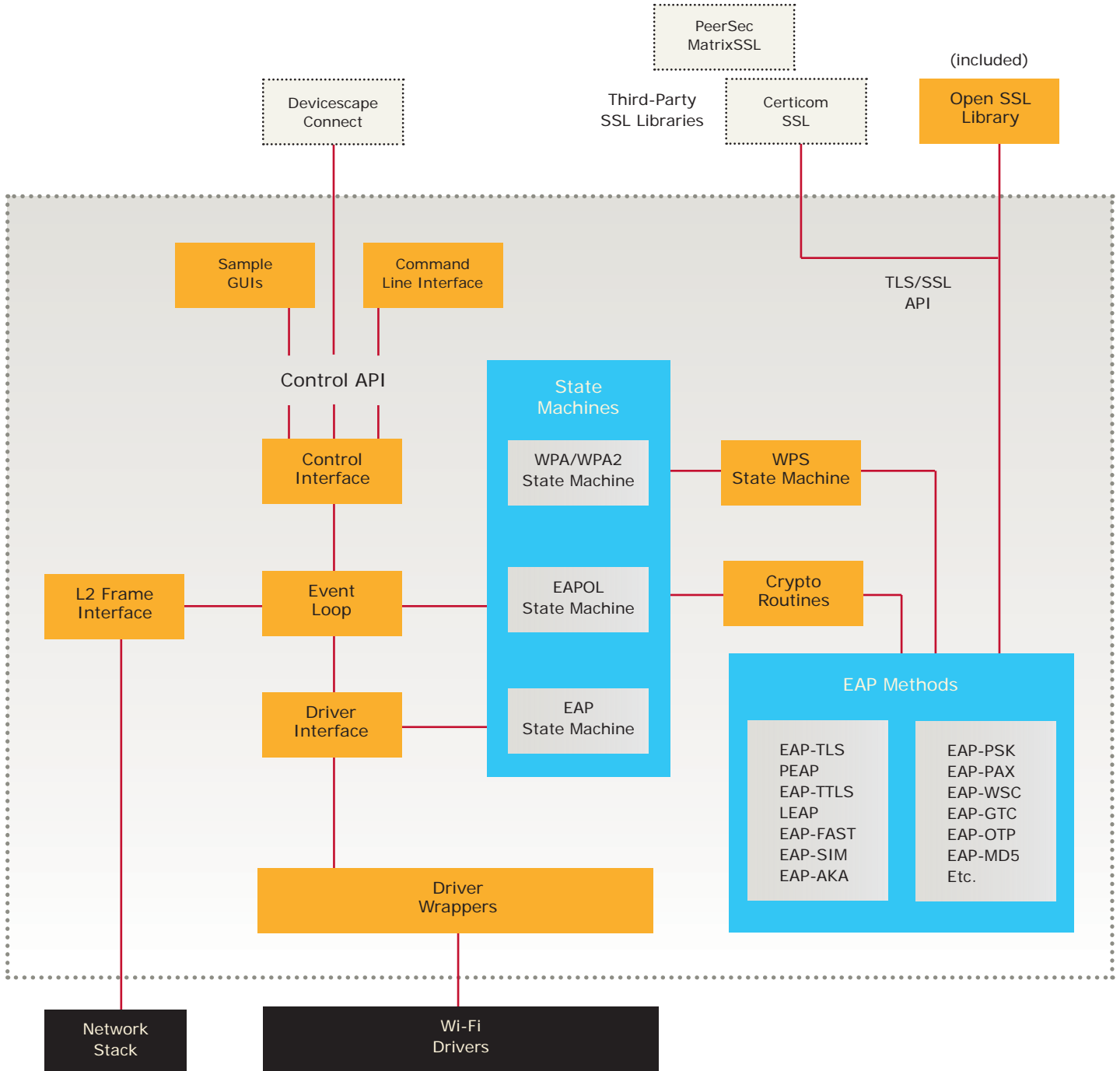
The Devicescape Agent supplicant integrates seamlessly with the award-winning Devicescape Connect solution. The Devicescape Connect solution enables seamless connectivity to public and commercial hotspots, in conjunction with the Devicescape Connect Service. Devicescape

Connect has been deployed on over 10 operating systems and is considered by industry and analysts to be a de rigeur feature on converged handsets and other leading edge consumer wireless devices. By combining the Devicescape Agent Supplicant with Devicescape Connect, you are assured of the smoothest integration, fastest time to market and best possible consumer connectivity experience.

Device Design Flexibility

The Devicescape Agent is written in standard ANSI C, and full source code is delivered to licensed customers. This gives device developers complete flexibility in porting the supplicant to the device operating system, processor, and wireless chipset of their choice. The Devicescape Agent has been successfully deployed on Linux, Windows XP/2000/Vista, Windows CE, Windows Mobile, Palm OS, VxWorks, ITRON, ThreadX and other operating systems. The product comes with build utilities and integration code for Linux 2.4 & 2.6, Windows CE 5.0, Windows Mobile 5.0/6.0, and Windows XP. For Windows CE and Windows Mobile environments, the Devicescape Agent is supplied with an intermediate (IM) driver for the NDIS stack, a sample GUI, and is architected to co-exist cleanly with the Microsoft Wireless Zero Config supplicant. A sample GUI is also provided for Linux and Windows XP. For Windows Vista, the Devicescape Agent interoperates with Vista Native Wi-Fi and NDIS6 directly. Extended EAP types are implemented using the EAPHost plug-in interface provided by Native Wi-Fi.

Devicescape Agent Architecture



Wireless Networking Features

IEEE / WI-FI WIRELESS STANDARDS

- IEEE 802.11 a / b / g / n
- IEEE 802.11i with RSN pre-authentication roaming
- IEEE 802.1X
 - Wireless & Wired
- WPA / WPA2
 - Personal & Enterprise
- Wi-Fi Extended EAP modes
- Wi-Fi Protected Setup
 - Enrollee & Registrar functionality
 - Pushbutton & PIN methods

WIRELESS LAN SECURITY FEATURES

- WEP (64 / 128-bit)
- Dynamic WEP with 802.1X
- IEEE 802.11i, WPA, WPA2
 - Personal and Enterprise
 - TKIP and AES (CCMP)
- Full IEEE 802.1X EAP support
- Smartcard

EAP METHODS

- EAP-TLS
- EAP-PEAP (PEAPv0 & PEAPv1)†
 - MSCHAPv2
 - TLS
 - GTC
 - OTP
 - MD5-Challenge
- EAP-TTLS†
 - EAP-MD5-Challenge (wired)
 - EAP-GTC
 - EAP-OTP
 - EAP-MSCHAPv2
 - EAP-TLS
 - MSCHAPv2
 - MSCHAP
 - PAP
 - CHAP

- LEAP
- EAP-MD5-Challenge
- EAP-MSCHAPv2
- EAP-GTC
- EAP-OTP
- EAP-SIM
- EAP-AKA
- Draft standard and Cisco-enhanced EAP-FAST
- EAP-WSC
- EAP-PAX
- EAP-PSK

CISCO COMPATIBLE EXTENSIONS (CCX)

- CCXv4 and v5 supplicant support
- KeyLabs certified Support for Funk and Meetinghouse OIDs

RADIUS SERVER VALIDATION

- Cisco ACS Server 4.0
- Cisco/Meetinghouse Aegis 1.1.6
- Juniper/Funk SBR Server 5.0.3
- Funk Odyssey Server 2.01
- Microsoft IAS Server 2003

MIB INSTRUMENTATION

- dot1x and dot11 MIBs
- Requires integration with customer SNMP agent

OTHER WIRELESS NETWORK FEATURES

- Simultaneous use of different Wi-Fi drivers
- Infrastructure and ad-hoc networks
- Preference lists

Platform Features

USER INTERFACES

- Sample GUI for Linux, Windows Mobile, WinCE, and Windows XP
- Command Line Interface

DEVELOPMENT SUPPORT FEATURES

- Extensive debug support
- EAP testing tool (Linux only)
- RSN pre-authentication tool (Linux only)
- API and configuration guide
- OS porting guide

SSL/TLS LIBRARIES

- OpenSSL (included)
- Certicom SSL validation
- PeerSec Networks MatrixSSL validation

PRE-INTEGRATED OPERATING SYSTEMS

- Linux 2.4 & 2.6
- Windows CE 5.0
- Windows Mobile 5.0/6.0/6.1
- Windows XP
- Windows Vista

VALIDATED WI-FI CHIPSETS

- Atheros AR52xx, AR600x
- Broadcom BCM4318, BCM4320
- Conexant Phaser, Voyager
- Intel 2915, 3845
- Marvell 88W8385, 8388, 8686
- NXP Semiconductors BGW211
- TITNET1251, 1253
- Easily ported to other Wi-Fi chipsets

PORTABILITY

- Full ANSI C source code provided
- Portable to any operating system
- Portable to any hardware environment
- Compatible with all Wi-Fi chipsets

MEMORY FOOTPRINT

- 150 KB flash for base configuration
- Add approximately 200 KB flash for tunneled EAP modes—EAP-TLS, EAP-TTLS, PEAP and EAP-FAST
- Add 70 KB flash for Wi-Fi Protected Setup
- 100 KB RAM during operation

DOCUMENTATION

- Release Notes
- Getting Started Guide
- Developer Guide
- API Reference Manual

CONNECT COMPATIBLE

- Devicescape Connect
- Devicescape Connect Service

Revised May 2008

† For the tunneled EAP methods, the mode used by the server to authenticate itself and establish a tunnel is listed as the first-level bullet; the modes used by the client to authenticate itself are shown as sub-bullets.