wave®

EMBASSY® Authentication Server

Multifactor Authentication: TPM, Smart Card, Biometric and Password for Windows Environment

Embassy Authentication Server (EAS) provides centralized management, provisioning and enforcement of multifactor domain access policies. With EAS, authentication policies can be based on Trusted Platform Module (TPM) credentials, Smart Card credentials, user passwords and fingerprint templates.

All major PC manufacturers ship PCs with embedded TPM hardware. Embedded TPM hardware provides secure storage and secure transactions for PKI credentials. TPM-based authentication with EAS combines secure hardware-embedded client credentials for the client PC platforms with strong multifactor credentials for users.

Multifactor authentication without complexity

EAS from Wave Systems is seamlessly integrated with Windows Domain Controller and Active Directory. EAS supports powerful combinations of:

- TPM credentials
- Smart Card credentials
- Biometrics
- Passwords

EAS is transparent by design and integrated with the Microsoft management and reporting utilities:

- Easy to install and easy to manage
- Extensive auditing and logging capabilities
- Standard Kerberos system 5.0 extensions
- Compliant with TCG standards

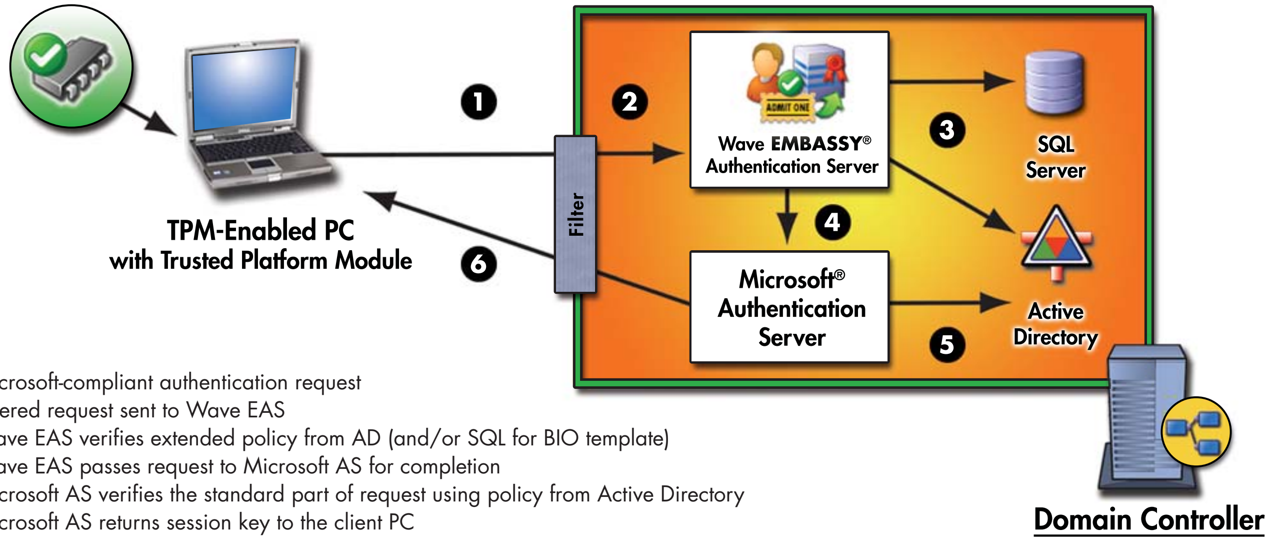
Key Features

- Domain server for hardware-based multifactor authentication.
- Centralized validation of TPM, biometric and password credentials.
- TPM-protected credentials for client PC platform authentication.

Integrated biometric authentication

Increasingly notebooks and PCs come with embedded fingerprint sensors. EAS makes it easy to incorporate the convenience of embedded biometrics into the business infrastructure. EAS is preconfigured to provide server-based biometric authentication. Powerful authentication policies can be provisioned and managed from the Domain Controller. EAS has an integrated biometric template capability with support for a variety of 3rd-party vendors.

EMBASSY Authentication Server Technical Overview


1
2
3
4
5
6
Filter
ADMIT ONE
Wave EMBASSY® Authentication Server
SQL Server
Microsoft® Authentication Server
Active Directory
TPM-Enabled PC with Trusted Platform Module
Domain Controller

1. Microsoft-compliant authentication request
2. Filtered request sent to Wave EAS
3. Wave EAS verifies extended policy from AD (and/or SQL for BIO template)
4. Wave EAS passes request to Microsoft AS for completion
5. Microsoft AS verifies the standard part of request using policy from Active Directory
6. Microsoft AS returns session key to the client PC

EMBASSY® Authentication Server

Management

EAS provides centralized management and enforcement for robust combinations of multifactor authentication. EAS policies can be managed through the standard Group Policy Object (GPO) editor. The management functions include:

- Editing/specifying policies for the group and the organizational unit level
- Enabling the biometric engine
- Specifying template storage
- Specifying audit/log attributes

Provisioning

EAS enables provisioning of role-based multifactor authentication policies at the group level. The following combinations are supported:

- Password only
- PKI only (Smart Card or TPM)
- Biometric only
- PKI or Password
- Biometric or Password
- PKI and Biometric
- Biometric and Password

Support for multiple Biometric template formats can be provisioned. This provides centralized server-based biometric template matching for clients that have incompatible biometric formats.

EAS Technical Specifications

Server OS

- Windows 2003

Authentication

- Kerberos 5.0
- Up to 2048 Bits RSA signature
- Microsoft Active Directory

Factors

- PKI Certificates (Smart Card, TPM)
- Passwords
- Biometric templates

Management Console (MMC)

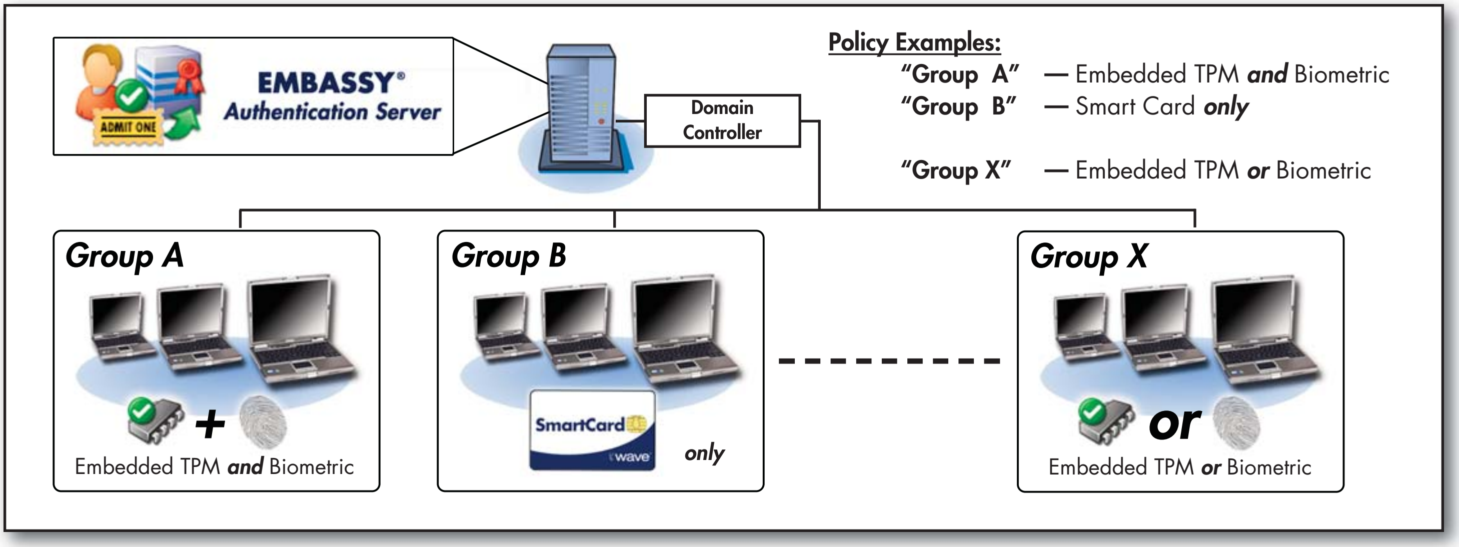
- Centralized management
- Microsoft GPO
- Role/group-based provisioning
- Microsoft event logger

Compliance

- Kerberos 5.0
- Challenge/response: ANSI X9.9
- Key Management: ANSI X9.17
- PKI X.509
- TPM 1.1, 1.2

Performance & Availability

- Integrated authentication load balancing for up to 50 servers
- Authentication transaction level balancing
- High availability; automatic failover for continuous uptime



Policy Examples:

"Group A" — Embedded TPM ***and*** Biometric
"Group B" — Smart Card ***only***

"Group X" — Embedded TPM ***or*** Biometric

Wave Systems solves the most critical security problems for enterprises and government with solutions that are trustworthy, reliable and easy-to-use while offering a speedy return on investment. Wave's trusted computing solutions include strong authentication, data protection, advanced password management and enterprise-wide trust management services.
Please visit www.wave.com. Part # 03-000174/version2.01

The Trusted Computer Group (TCG) is a new industry group dedicated to embedding trust and security more broadly into computing platforms and devices. The TCG will work to create open standards that can be adopted for use in products and solutions across the spectrum of computing, including devices beyond the PC, to enable secure and trustworthy computing that can protect data, privacy and individual rights.

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238
tel (877) 228-WAVE • fax (413) 243-0045