Entrust Datacard™

Arthatel
security.system@arthatel.co.id
www.arthatel.co.id

Entrust Authority Security Manager

Managing an In-House Certification Authority with Ease

Digital certificates allow organizations to leverage encryption and digital signatures to support a variety of security services, including user and device authentication, transaction integrity and verification, and data security.

Entrust Authority Security Manager, the world's leading public key infrastructure (PKI), helps these organizations easily manage their security infrastructure, and allows easy management of the digital keys and certificates that secure user and device identities.

Simplified Certificate Management

Deployed at the server-level, Entrust Authority Security Manager software enables valuable security capabilities — including permission management, digital signature, digital receipt and encryption — to be applied across a wide variety of enterprise applications.

▶ entrust.com/PKI

Mobile Security

Mobile operating systems inherently have the ability to store certificate-based credentials and make them available to applications that run on the device— such as VPN clients and email software. Entrust Authority Security Manager issues certificates to mobile devices, enabling organizations to efficiently protect their mobile network.

An ePassport Foundation

Entrust Authority Security Manager is a mandatory component of every Entrust ePassport system. The solution may be configured as a CSCA, CVCA or DV to issue certificates used to secure ePassports. Entrust also offers a variety of complementary components that help streamline the ePassport ecosystem.

▶ entrust.com/epassport

Easy & Transparent

Automatic and transparent key and certificate management means users do not need to know anything about security. The platform even provides key history, backup and recovery features so organizations have confidence encrypted information will not get lost if users misplace their keys.

+1-888-690-2424

entrust@entrust.com
entrust.com/PKI

@EntrustDatacard
+entrust
/EntrustVideo
/EntrustSecurity

DOWNLOAD
THIS
DATA SHEET

Product Benefits

- Manage digital identities within an organization for company-wide security, without burdening administration
- Simplify the user experience; users do not need to understand public keys and certificates to add security to communications, mobile devices and transactions
- Enforce corporate-wide security policies relating to passwords, administration and digital certificate settings
- Offers high levels of interoperability, including enhanced integration with Microsoft software to help customers leverage existing investments
- Identify, manage and authenticate mobile devices used on the corporate network

Seamless and Transparent Security Management

Entrust PKI products and services reduce end-user help-desk calls.

Tight Integration

Generate certificates for mobile devices as requested by Entrust Authority Administration Services or the Entrust IdentityGuard software authentication platform. Both solutions provide a common Web service interface for enrolling and managing certificates issued to mobile devices.

Secure Storage

Store the CA private key securely to ensure the integrity of your in-house CA infrastructure. The solution also maintains an auditable database of users' private key histories for recovery purposes.

Easy Certificate Issuance

Issue certificates for users, applications or devices, including tablets and smartphones, which support the X.509 certificate standard.

CRL Control

Publish certificate revocation lists (CRLs) that are used to verify whether a user or application's certificate is still trusted by the CA that issued it.

End-User Convenience

Leverage an advanced security infrastructure that accommodates users who log in from different workstations, work offline or from mobile devices, or use various methods of authentication (e.g., smartcards, tokens or biometric devices).

Perfected Automation

Take advantage of the solution’s automated key and certificate lifecycle management capabilities. Users do not need to know anything about public keys and certificates to add security to communications, devices or transactions.

Optional Enhancements

Leverage Entrust Authority Security Manager's optional components. Organizations have the option to add further security management capabilities — including automated enrollment, self-registration and self-recovery of digital identities and secure roaming.

Complementary Entrust Products

Entrust Entelligence Security Provider

This thin-client desktop security software allows organizations to use a single digital identity to add security capabilities beyond authentication to applications such as email or file encryption.

Entrust Authority Administration Services

This component provides Web-based applications and services that interact with Entrust Authority Security Manager to manage digital IDs and certificates. Services include administration interfaces that allow administrators to manage users and certificates, and enrollment services that allow users and non-human entities (e.g., computers and mobile devices) to enroll for certificates. Entrust Authority Administration Services also enables auto-enrollment of users and machines.

Entrust Authority Roaming Server

Roaming Server adds mobility to the enhanced security capabilities of the Security Manager system. The server provides users with secure access to digital content from any location without the need for users to carry the digital IDs required to establish secure connections.

Entrust Authority Security Manager Proxy

Security Manager Proxy allows the operation of Security Manager over the Internet using standard Internet protocols without making changes to existing firewall settings.

Entrust Authority Toolkits

Entrust Authority toolkits provide a common set of services that permit developers to deploy applications that solve business problems without having to spend valuable development cycles creating these common services.

Entrust Entelligence Messaging Server

This appliance-based email security solution delivers comprehensive, standards-based email encryption capabilities, simplifying secure communication with external business partners and customers.

Entrust GetAccess

This scalable Web access management solution provides authorization and sign-on capabilities to Web applications. Entrust GetAccess employs dynamic, context-sensitive policies to control user access to company resources.

Technical Features

- Automated digital ID management including updates, revocation and recovery
- Support for unlimited administrators and up to 10 million users per CA
- Web-based administration for delegated and distributed administrative processes available via optional Administration Services component
- Centrally managed policies and controls
- Certified for Federal Information Processing Standards (FIPS) 140-2 Level 2
- Common Criteria EAL 4+ certified
- Comprehensive and customizable auditing and reporting
- Support for peer-to-peer and hierarchical cross-certification of CAs
- Support for standards including X.509 certificates and CRL formats, PKIX-CMP, PKCS#7/10 and SCEP (via Entrust Enrollment Products); provides interoperability with PKI-aware applications such as virtual private networks, Web browsers, VPN devices, mobile devices, email and business applications
- Interoperability with LDAP directories (including Microsoft Active Directory), smartcards, OCSP responders and hardware security modules (including SafeNet and Thales)

Platforms Supported

- Entrust Authority Security Manager is available for deployment in Microsoft® Windows®, UNIX and Linux environments.
- Microsoft® Windows® Server 2008 R2 (Entrust PostgreSQL 8.3.11 database)
- Oracle® Solaris 10 (Entrust PostgreSQL 8.3.11, Oracle Database 10G R1/R2 or Oracle Database 11G R1/R2 database)
- HP-UX 11.31 (Entrust ProstgreSQL 9.0.7)
- Red Hat Enterprise Linux 5.4 or later versions of 5.x (Entrust PostgreSQL 8.3.11 database)
- Red Hat Enterprise Linux (6.0-6.2)

About Entrust Datacard
Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information about Entrust products and services,
email **security.system@arthatel.co.id** or visit **www.entrust.com**

Arthatel

PT. Artha Telekomindo
Parc 18, Tower A, 3rd & 4th Floor
Sudirman Central Business District (SCBD)
Jl. Jenderal Sudirman Kav 52-53
Jakarta 12190 - Indonesia
Phone: +62 (021) 515 0000
Fax: +62 (021) 515 0006
Call Center: +62 (021)2552 5100
www.arthatel.co.id

Headquarters
Entrust Datacard
1187 Park Place
Shakopee, MN 55379
USA

Entrust Datacard™