

Overview

The DS3 Authentication Server Solution is the complete 2-factor authentication solution to provide end-to-end security for passwords & highly sensitive information to secure electronic transactions.

Applications such as Internet/Phone Banking, Stock Trading and remote ASP services require this enhanced security for protection against cryptographic and Trojan attacks.

Solution features include: a powerful cryptographic engine; GUI administration; a full-fledged token management system for all combinations of 2nd factor hardware tokens, SMTP/SMS and Software J2ME and PC tokens.

For more information, please contact DS3 at:

URL:
<http://www.ds3global.com>

Email:
info@ds3global.com



Phone: +65 64795688

Fax: +65 64795488



Key Components

- DS3 Authentication Server
- Java RMI over SSL
- Radius Server
- Support for hardware, software, Messaging (SMS) tokens.
- Embedded software HSM
- Optional FIPS 140-2 Hardware HSM

DS3 Authentication Server (DSX – 100)													
DS3 Authentication Server (DSX – 100)	<ul style="list-style-type: none"> •19" 2U EIA Rack-Mount Server •2 x Intel XEON Quad Core CPU •4 GB RAM •1 x 73 GB Hard disk (RAID 0) – Operating System •2 x 73 GB Hard disk (RAID 1) – Application Data •Browser GUI Administration •Java RMI Server over SSL •RADIUS Server •Embedded software HSM •Embedded Database •Gigabit Ethernet connectivity •Hardened OS with built in packet-filtering Firewall 												
Performance	<ul style="list-style-type: none"> •100 end-to-end Auth/sec •Support up to 5,000,000 users •2500 Concurrent Login Sessions •200 OTP Auth/sec •100 RSA-1024 decrypt/sec 												
Vendor Client Supported	<ul style="list-style-type: none"> •All RADIUS Compliant clients •VPNs •Microsoft IIS •Oracle WebLogic •SunOne Glassfish server •IBM WebSphere •Apache Tomcat •TAMeb WebSeal server 												
Security Package													
Supported Token	<table border="0"> <tr> <td>Hardware tokens Supported:</td> <td>Soft Tokens Supported:</td> </tr> <tr> <td>•OATH HOTP & TOTP</td> <td>•J2ME Midlet on MIDP 1.0</td> </tr> <tr> <td>•VASCO Digipass</td> <td>•iPhone</td> </tr> <tr> <td>•RSA SecurID</td> <td>•Windows EXE</td> </tr> <tr> <td>•PKI X.509 Certificates</td> <td>•Java Applet in JVM1.5</td> </tr> <tr> <td>•EMV CAP (w H/W HSM Only)</td> <td>•Android</td> </tr> </table> 	Hardware tokens Supported:	Soft Tokens Supported:	•OATH HOTP & TOTP	•J2ME Midlet on MIDP 1.0	•VASCO Digipass	•iPhone	•RSA SecurID	•Windows EXE	•PKI X.509 Certificates	•Java Applet in JVM1.5	•EMV CAP (w H/W HSM Only)	•Android
Hardware tokens Supported:	Soft Tokens Supported:												
•OATH HOTP & TOTP	•J2ME Midlet on MIDP 1.0												
•VASCO Digipass	•iPhone												
•RSA SecurID	•Windows EXE												
•PKI X.509 Certificates	•Java Applet in JVM1.5												
•EMV CAP (w H/W HSM Only)	•Android												
End-to-End Encryption	<ul style="list-style-type: none"> •RSA-1024 E2E Encryption •3DES / AES Encryption / Decryption •SHA1/256/512 •Remote Digital Signature 												