SecureMetric Technology

ST3 Ace

SECURE METRIC TECHNOLOGY

Simplify PKI token deployment as to achieve

excellent user experiences.

ST3 ACE is aimed to be bundled with SecureMetric's patterned advanced SecureTMS client components that in order to simplify PKI token deployment as to achieve excellent user experiences.

The key challenge for most PKI implementation is user experience management, this usually considered as one of the key success factor. If the user needs to go through all the tedious PKI processes without proper, the chances to encounter strong user resistant will be very likely. A great PKI implementation should come with well designed user friendly approach to simplify PKI processes as much as possible while still complying to the set security policies.

FIPS VALIDATED 140-2 LEVEL 3   COMMON CRITERIA LEVEL 2   myCC

Certified

ST3 Ace the latest innovation by SecureMetric Technology is designed to integrate all critical token management functionalities and certificate lifecycle to the middleware level without interaction with web browsers. In addition to that, almost every PKI processes can now be automated without heavily involving end users.

Implementation of ST3 Ace will only require backend integration to existing Registration Authority (RA) software with internet/ intranet connectivity between end users and the RA software.

Typical PKI problems can now be solved with ST3 Ace:

Supporting

• Difficulty on supporting multiple platform
The ST3 Ace online installer can now cross-platform supporting Windows, Linux & Mac without breaking a sweat.

Unblocking

• Forgetting Token User PIN after long holiday which resulted a tedious unblocking process or even sending the physical token back to the provider
Secure Token User PIN Unblocking mechanism from ST3 Ace not only simplifies the PIN Unblocking process, but also allowing end users to perform such function remotely.

• Tedious Certificate Enrollment Process via Online Enrollment Portal
Certificate Enrollment via ST3 Ace eliminates the

Enrollment

need of data entry from end user side with the end user only needs to verify necessary information before certificate enrollment take place.

Renewal

• Tedious Certificate Renewal Process via Online Renewal Portal
Auto Renewal is supported by ST3 Ace with even the possibility of using pre-configured renewal policy. Fully automated renewal is also possible.

Troubleshooting

• Technical Troubleshooting especially for non-IT background users
Diagnostic tool in the ST3 Ace is ready to provide revolutionary way of troubleshooting where most common problems can be resolved by the tool without even dialing the technical support number. In the event where further technical support is needed, this tool can produce a report which can be very useful for technical support to analyze the problem

Operate

• Annoying ActiveX/ Java Applet Components
Forget these web application components. The ST3 Ace can operate with full token and certificate functions without using any of these annoying components that requires client side installation and difficult to support.

Model	SecureToken ST3 ACE
Chip Security Level	Secure Microprocessor Smart Chip based with PBOC, CFCA, certified CCEALS+, Hongsi HS32
Processor	16-bit
Interface	CCID
Memory Size	128k (64K for User) on Smart Chip 2MB for Flash
Card Operating System	SecureCOS
Middleware	Microsoft CSP/CNG, Minidriver, PKCS#11
Windows Smart Card Logon	YES
Certificate Storage	Up to 16 (X.509 v3 Digital Certificate)
On-Board Security Algorithms	RSA (Hardware generated 1024/2048 bit RSA Key Pairs), ECDSA 192/256 DES/3DES, AES 128/192/256 bit, SHA1, SHA-2 (256, 384)
Dimension	59mm x 18mm x 9mm
Certification	CE, FCC, MYCC Level 2, FIPS Level 3 (FIPS 140-2 Level 3)
Weight	5g
Power Dissipation	< 250 mW
Operating Temperature	0 °C ~ 70 °C (32 °F ~ 158 °F)
Storage Temperature	-20 °C ~ 85 °C (-4 °F ~ 185 °F)
Humidity Rating	0 to 100% without condensation
Connector Type	USB 1.1, 2.0 full speed, Connector type A
Casing	Hard Molded Plastic, Tamper Prove (Optional), RoHS compliance
Memory Cell Rewrites	At least 500,000 write
Memory Data Retention	At least 10 years
Standards	X.509 v3 Certificate Storage, SSL v3, IPSec, ISO 7816 1-4 8 9 12, CCID, PC/SC
Supported Operating Systems	Windows XP/ Vista/ 7/ 8/ 10/ ... Windows Server, Linux, Mac OS