CRYPTOMATHIC
www.cryptomathic.com

v1.0

Crypto Service Gateway - PCI Compliance

THE PERFECT CRYPTO PLATFORM

Cryptomathic Crypto Service Gateway (CSG) is the perfect flexible and high-performance crypto platform on which to build new PCI-compliant processing systems or to adapt legacy systems for PCI compliance. CSG can help achieve PCI compliance in one of several ways:

- Acting as a data encryption/tokenization platform to help achieve encryption across a system and thus de-scope large parts of the system from PCI security rules
- Acting as the cardholder data environment and being the sole location (or one of a limited number of locations) where cardholder data is processed in clear
- Acting as a central point of policy control, protection and auditing for use of commands that access cardholder data (through crypto) in order to demonstrate proper security controls on access to data. CSG can be managed under dual control with 2FA and has full transaction logging and monitoring

CSG is flexible through supporting a variety of high-level data protection services that are easy to use and enable application developers to efficiently work with sensitive customer data while retaining it in a processable format. CSG offers the following tokenization and data obfuscation services:

- Parametric Data Tokenization – this is an adjustable tokenization mechanism which can draw its security from either format preserving encryption (FPE) or database storage, or a proportional mixture of both, yielding maximum security and compliance. CSG achieves this while also being flexible to accommodate infrastructure constraints (e.g. hardware and database platforms) and decentralisation constraints (running compatible tokenization at multiple data centres which are not close by), and is adjustable to be future-proof
- Character-set independent data "spinning" – this algorithm protects sensitive customer data such as names and addresses by applying a format preserving cipher to each character individually. Data structure such as alphabet, spacing, punctuation and letter case is unaffected. It can efficiently scramble large volumes of data in a CBC mode and includes an algorithm to deterministically extract a unique record IV from other mixed-format database columns or transaction metadata, which means it maintains good security without any data overhead
- Data masking – discarding of sensitive data value entirely while retaining the overall data structure, which is useful for creating representative test data sets out of live data

Tokenization services are well suited when applications must process or transport PCI sensitive data through third party networks or platforms, or when data storage overheads are at a premium, but often to achieve PCI compliance general purpose encryption facilities are a simpler and stronger approach, for instance for bulk storage of backup data containing PCI sensitive fields. CSG supports encryption with value added features to ease lifecycle management and transport concerns:

- Hybrid data encryption with RSA/AES – for data transport applications requiring full encryption, CSG offers hybrid RSA/AES or RSA/3DES encryption which offers the maximum protection for transmitted data and still retains the advantages of asymmetric crypto. CSG can act as the decryption endpoint and libraries can be distributed to encrypt data in a compatible format on a variety of platforms including Java/Javascript/C/C#

- Managed data encryption – for data transport applications requiring full authenticated encryption (encryption with confidentiality and integrity). Cryptomathic's open, peer-reviewed managed data encryption format offers confidentiality and integrity of data simultaneously while still only requiring a single HSM call per crypto operation (conventional schemes halve performance by requiring separate calls for MACing and Encryption)

- Conventional encryption – encryption in industry standard formats which are interoperable with legacy systems. CSG supports lowest common denominator formats such as ECB, CBC, IBM IPS and RSA PKCS#1 V1.5

CSG CRYPTO SERVICE EXAMPLES

Application developers integrate with CSG using Java, .NET or C++, and an interactive console is provided to test out commands written in 'Cryptographic Query Language' (CQL). Using crypto features in CSG is as easy as typing a command, for example:

```
DO ENCRYPT FROM App TO Database WITH DATA <insert
data here>
DO DECRYPT FROM Database TO App WITH DATA <insert
data here>

DO TOKENIZE FROM App TO Database:PAN WITH DATA
<insert data here>
DO DETOKENIZE FROM Database:PAN TO App WITH DATA
<insert data here>
(configurable parameters allow this tokenization to
exclude the first 6 and last 4 digits)

DO TOKENIZE FROM App TO Database:DLV WITH DATA
<insert data here>
(tokenization works on mixed digit/alphabet strings)

DO MASK WITH DATA <insert data here>

DO SPIN FROM App TO Database WITH DATA <insert data
here>
```