**FACT SHEET**

**NESA's UAE IAS**

How can Gemalto’s Data Protection and Authentication Solutions Help with Compliance?

---

**About NESA’s Mandatory Cryptography and Authentication Security Controls for the UAE**

To protect the UAE’s critical data information infrastructure and improve national cyber security, the National Electronic Security Authority (NESA), has produced the UAE Information Assurance Standards (UAE IAS), which is a set of standards and guidelines for government entities in critical sectors. Compliance with these standards is mandatory for all government organizations, semi-government organizations and business organizations that are identified as critical infrastructure to UAE.

NESA’s UAE IAS regulations were created with the aim to:

- Strengthen the security of UAE cyber assets and reduce corresponding risk levels
- Protect critical infrastructure
- Improve threat awareness in the UAE
- Develop human capital and technical capabilities

**NESA’s UAE IAS Control Structure**

NESA’s UAE IAS lists 188 security controls and standards which are grouped into four different tiers, ranging in priority from P1 (highest) to P4 (lowest). NESA created the list of security controls based on 24 threats that were compiled from various industry reports, and prioritized them based on the percentage of breaches that were found. Out of the 188 security controls listed, 39 of them are P1 controls which address 80% of the possible security threats NESA identified. Implementing P1 controls is an organization’s first step towards achieving compliance and building a strong information security foundation against cyberattacks.

---

**NESA’s Audit and Compliance Process**

NESA will also be operating on a tiered approach when enforcing UAE IAS compliance. The level of risk that an organization poses to the UAE’s information infrastructure (based on the organizations current security controls and the inherent risk of their industry), will determine how closely NESA and industry regulators will be working with them. Although NESA hasn’t yet outlined a mandatory compliance date for organizations, or any potential fines, these controls are required to be implemented by all the relevant entities, regardless of the outcome of their NESA Risk Assessment results. Notwithstanding any penalties and fines that NESA could enforce, organizations should start to implement P1 controls to protect against potential data breaches, and mitigate the associated financial and reputational losses.

---

**NESA’s Risk Assessment Framework**

<table>
<thead>
<tr>
<th>PROCEDURE</th>
<th>IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting</td>
<td>Maturity-based self-assessment by stakeholders in line with mandatory vs. voluntary requirement</td>
</tr>
<tr>
<td>Auditing</td>
<td>When appropriate, NESA can audit stakeholders by requesting specific evidence in support of self-assessment report</td>
</tr>
<tr>
<td>Testing</td>
<td>When appropriate, NESA can commission tests of information security measures in place at stakeholders</td>
</tr>
<tr>
<td>National Security Intervention</td>
<td>In extreme cases, NESA should be able to directly intervene when an entity’s activities are leading to unacceptable national security risks</td>
</tr>
</tbody>
</table>
UAE IAS Guidelines

We’ve extracted the following sections of the guideline to highlight the areas where Gemalto’s products can help protect your data and address NESA’s cryptography security controls and standards.

Apply secure encryption controls and build a strong crypto foundation with Gemalto’s SafeNet Identity and Data Protection Portfolio to comply with the following mandates:

- Cryptographic controls should be designed and implemented in a manner considerate of the Entity’s need to effectively monitor its information flow, retain oversight of information system usage and protect against malicious software (Control specification - IS.5.7)
- The Entity should have in place adequate provisions for key management of cryptographic systems including issuing, changing and revoking keys as necessary (Control specification - IS.5.8)
- The Entity should endeavor to only select robust public-domain (non-proprietary) cryptographic algorithms for use within its information systems and networks. Where requirements and/or market constraints present a strong case for the use of proprietary cryptographic algorithms, the proposed use should be discussed in advance with ADSIC (Control specification - IS.5.2)
- For data hosted at Entity-owned facilities, cryptographic protection should be applied to data at rest (Control specification - IS.5.9)
- Data hosted at non Entity-owned facilities e.g. third-party data centers should be subject to strong encryption protection at rest (Control specification - IS.5.10)
- Data transmitted to/from non-Entity-owned facilities e.g. third-party data centers should be subject to strong encryption to protect data in motion (Control specification - IS.5.11)
- Workflow approval within information systems should be supported via the use of digital signatures using public key cryptography (Control specification - IS.5.12)
- The Entity should employ gateway-to-gateway strong encryption to protect data traffic transiting between its physical locations, to limit the potential for eavesdropping (Control specification - IS.11.1)
- Data of classification ‘Confidential’ or above transiting over a wireless network should be subjected to strong encryption to protect its confidentiality (Control specification - IS.12.6)

Enforce strong access controls with Gemalto’s SafeNet Authentication Solutions to comply with NESA authentication mandates:

- An automatic authentication method (e.g. badge reader) should be deployed for access to the data center perimeter. The Entity should consider supplementing this with a second form of authentication (e.g. biometric, key pad PIN) for access to computer rooms (Control specification - PE.4.9)
- Two factor authentication (for example leveraging elements that include challenge-response security tokens or biometric-based systems) should be used to improve authentication mechanisms for remote access connections. Security tokens may be hardware or software based (Control specification - IA.5.10)

How can Gemalto help you comply with NESA’s UAE IAS Regulations?

Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions – from the edge to the core. Gemalto’s portfolio of SafeNet Identity and Data Protection solutions enables enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.
SafeNet KeySecure – Secure Key Management and Cryptographic Processing

Centrally manage your cryptographic processing, encryption keys and ultimately own your data with SafeNet KeySecure. Whether it’s stored in a database, file server, application, traditional or virtualized data center, or public cloud environment, your sensitive data is secure from compromise. SafeNet KeySecure simplifies the management of encryption keys across the entire lifecycle including secure key generation, storage and backup, key distribution, deactivation and deletion. Organizations can also automate policy driven operations, which simplifies tasks like key expiry and rotation, which are requirements of NESA’s UAE IAS regulation.

Additionally, SafeNet KeySecure provides detailed logging and audit tracking of all key state changes, administrator access and policy changes. Audit trails are securely stored and signed for non-repudiation and can be consumed by leading 3rd party SIEM tools. Using SafeNet KeySecure, organizations can centrally manage multiple key types, including Symmetric and Asymmetric Keys, secret data, and X.509 certificates along with associated policies.

SafeNet Data Protection Connector Portfolio – Secure Your Data at Rest

Coupled with SafeNet KeySecure, the SafeNet Data Protection Connector portfolio keeps administrators in full control of their data wherever it is resides and however it is used. In turn, this level of control keeps organizations compliant with UAE IAS.

Gemalto’s SafeNet Data Protection Connector Portfolio offers a comprehensive range of encryption and tokenization solutions to secure data-at-rest and data-in-motion across organizations regardless of their operational or IT architecture. Our file system-level, database column-level, application-level encryption, virtual machine full disk encryption, and both vaulted and vaultless tokenization solutions can secure data at any point in its lifecycle from creation to storage. With such a vast array of options, organizations can address a wide range of challenges from simply encrypting data that stays at rest to encrypting data and ensuring that only ciphertext is ever transmitted across the network or even outside the organization. These solutions are cloud agnostic – meaning they will work in any public or private cloud, as well as in any virtualized environments.

SafeNet High Speed Encryptors – Secure Your Data in Motion

SafeNet High Speed Encryptors from Gemalto provide proven high-assurance Ethernet network security for your sensitive data on the move from data center or site to site, or multiple sites, to back up and disaster recovery, to the last mile, on-premises, up to the cloud and back again.

SafeNet certified network encryption devices offer the ideal solution for data in motion security, including time-sensitive voice and video streams, for government organizations and enterprises that need to conform to the most stringent compliance requirements, including NESA’s mandate.

A powerful safeguard for data in motion, SafeNet High Speed Encryptors deliver high-assurance certified Layer 2 encryption capabilities that meet secure network performance demands for real-time low latency and near zero overhead to provide security without compromise for data on the move across the network up to 100 Gbps.

SafeNet Luna HSMs – Secure Root of Trust for Your Data

Easily conform to NESA’s mandates with SafeNet Luna HSMs from Gemalto. Ensure your data is safe from a cyber-attack by storing your private cryptography keys inside a hardened, tamper-resistant, FIPS-validated device. Without access to the keys, data is rendered useless. Your organization will benefit from Gemalto’s years of experience, and stringent product verification testing that certifies the security and integrity of our devices.

IDPrime Converged Badge – Secure Physical and Logical Access with a single Credential

Gemalto offers combined authentication solutions to meet NESA’s mandates for controlled access to the data center perimeter, as well as two-factor authentication for remote access connections. Gemalto’s wide range of smart cards provide combined logical and physical access controls. Our portfolio includes contact cards with a wide choice of card body options and contactless technologies, as well as dual interface cards that are compatible with NFC. Gemalto integrates with a very long list of physical access solutions including MIFARE, DESFire, HID, which allows you to use existing physical access systems and readers. The convergence of logical (LAC) and physical (PAC) access into one credential significantly reduces costs of badge deployment, while providing a convenient solution for users.
ABOUT GEMALTO’S SAFENET IDENTITY AND DATA PROTECTION SOLUTIONS

Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of digital identities, transactions, payments, and data – from the edge to the core. Gemalto’s portfolio of SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com
Follow Us: blog.gemalto.com/security