**SmartCard-HSM** is a light-weight hardware security module for secure key generation and storage. It has been designed for PKI and cryptographic systems with low to moderate load. The unique build in support for card verifiable certificates as defined in TR-03110 (Extended Access Control) makes a SmartCard-HSM the perfect choice for storing key material in an EAC-PKI. A trusted channel and public key attestation allow remote key generation and certificate issuance.

**FEATURES**
- Supports RSA and ECDSA
- Authenticated certificate signing requests as per TR-03110
- Chip authentication and secure channel as per TR-03110
- ISO 7816-4 command interface
- User PIN 6 – 16 bytes
- Standardized and proprietary domain parameters for ECC
- Common Criteria EAL 5+ certified operating system

**ALGORITHMS**
- RSA PKCS#1 V1.5/PSS with SHA-1/SHA-224/SHA-256
- ECDSA GF(p) with SHA-1/SHA-224/SHA-256

**KEY SIZES**
- RSA with 1024, 1536 and 2048 bits
- ECC with 192, 224, 256 and 320 bits

**PERFORMANCE**

### Key Generation with authenticated public key export

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>On-Card with Export per minute</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA 1024</td>
<td>10</td>
</tr>
<tr>
<td>RSA 1536</td>
<td>5</td>
</tr>
<tr>
<td>RSA 2048</td>
<td>2</td>
</tr>
<tr>
<td>ECC GF(p) 256</td>
<td>10</td>
</tr>
</tbody>
</table>

### Signature creation

| Algorithm       | Off-Card Hash per minute | On-Card Hash per minute *|)
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA 1024</td>
<td>350</td>
<td>125</td>
</tr>
<tr>
<td>RSA 1536</td>
<td>200</td>
<td>100</td>
</tr>
<tr>
<td>RSA 2048</td>
<td>100</td>
<td>68</td>
</tr>
<tr>
<td>ECDSA GF(p) 256</td>
<td>360</td>
<td>125</td>
</tr>
</tbody>
</table>

*) SHA-256 with 1kb data

**MEMORY CAPACITY**
- Up to 60 ECC GF(p) 256-bit keys or
- Up to 48 RSA 2048-bit keys or
- 55Kb in up to 50 elementary files

---

www.smartcard-hsm.com