Gemalto Mobile ID Smart App

Product Description

Gemalto Mobile ID Smart App was introduced to meet the growing market requirements for an advanced smartphone user experience for online services that does not compromise on security. The app allows citizens to authenticate to websites, confirm transactions and perform electronic signatures with convenience and ease. It stores the digital identity of the mobile user and ensures that their digital credentials stay protected and secure at all times.

Deployment model

> Available as an app or Software Development Kit (SDK)
> Gemalto Mobile ID Smart App: customizable UI with specific branding [skin and logo] to comply with customer’s guidelines and localization to preferred language
> Gemalto Mobile ID Smart SDK: allows easy integration of the Gemalto Mobile ID Smart features in any customer application

Security

> Out-of-Band communication to mitigate single channel risks
> Built on Gemalto Mobile Security Core with advanced protection against malware and corrupted devices
> Obfuscation of sensitive code to protect from reverse engineering and hacking
> RASP protection
  • Jailbreak/Root detection
  • Jailbreak/Root hiding tools detection
  • Anti-Hooking
  • Anti-Debug
  • Static Anti-Tampering
  • Anti-Emulator
  • Dynamic Anti-Tampering
> Gemalto Secure PIN pad enabling scrambled layout and eliminating the need for PIN value to be stored in device RAM
> Configurable PIN validity policies [e.g. non-uniformity, no ascending/descending order, no forbidden combinations, etc.]
> Secure encrypted storage
  • Uses asymmetric encryption to protect the keys and credentials
  • Encryption keys are diversified by device and application fingerprints and protected by PIN
**Technical Data Sheet - Gemalto Mobile ID Smart App**

**Communication**
- TCP/IP based secure communication with Gemalto Digital Identity Service back-end platform
- Uses TLS protocol and additional end-to-end secured and encrypted communication
- Session and integrity keys for secure communication generated for every request and deleted when response received
- Communicates either with push messages or by polling the back-end to receive the request

**User experience**
- Supports a wide range of authentication methods
  - PIN, pattern, facial with liveness detection, fingerprint
- User can switch from one authentication method to another
- Logging and browsing of main operations
- Multi-device support

**Back-end platform**
- Managed by Gemalto Digital Identity Services back-end platform (end-user registration, device association, PKI key generation, authentication, signature processes, etc.)
- Authentication using SAML 2.0, Open ID Connect 2.0
- Signature using OASIS DSS, compliant with eIDAS Qualified Electronic Signature (QES)
- GDPR compliant – based on data minimization, data protection, pseudonymization, anonymization, user’s data and consent management
- Self-Care and Customer Care Portals/APIs for Mobile ID Smart App lifecycle management

**Enrollment**
- Supports remote Identity Proofing through:
  - eID, ICAO based electronic documents
  - Non-electronic identity documents
  - Biometric identification
  - QR code scanning or URL based registration

**Authentication**
- Mobile ID Smart App standalone: eIDAS Substantial, NIST AAL 2, ISO LoA 3
- Mobile ID Smart App + NFC eID card + PIN: eIDAS High, NIST AAL 3, ISO LoA 4
- Mobile ID Smart App + ICAO doc + Face Recognition: eIDAS High, NIST AAL 3, ISO LoA 4

**Digital Signature**

**Levels**
- Mobile ID Smart App standalone: eIDAS Advanced Electronic Signature (AES)
- Mobile ID Smart App + NFC eID card + PIN: eIDAS Qualified Electronic Signature (QES)

**Formats**
- Sign Hash (PKCS#1/CAdES-BES) – Document Signing
  - XML (xmlDsign)
  - PDF (in fact binary or XML embedded in PDF document)
  - ASIC - Signature associated to zip container
- Sign Text (PKCS#7/CMS/CAdES-BES) – Text Signing

**Key Management features**
- On-Board Key Generation (OBKG): Generated in the app using a crypto engine, stored in the app’s encrypted secure storage
- Mobile PKCS#10 registration and certification request
- Supports multiple keys

**Cryptography**
- RSA: 2048-bit key and longer
- ECC: ECDSA 256-bit key and longer
- SHA-256, SHA-512

**Mobile OS covered by default**
- Android 5.0 and above
- iOS 10.0 and above
# Technical Data Sheet - Gemalto Mobile ID Smart App

## Value Added Functionality as Options
Combining Mobile ID and Electronic Identity Documents
Works with Gemalto Mobile Link

<table>
<thead>
<tr>
<th>SPECIFICATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Applications</td>
</tr>
<tr>
<td>Communication</td>
</tr>
<tr>
<td>Authentication</td>
</tr>
<tr>
<td>Digital Signature</td>
</tr>
<tr>
<td>Identity Proofing</td>
</tr>
</tbody>
</table>

Combining Mobile ID and non-electronic Identity Documents
Works with Gemalto Remote Identity Verification Solution

<table>
<thead>
<tr>
<th>SPECIFICATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Cards</td>
</tr>
<tr>
<td>Communication</td>
</tr>
<tr>
<td>Identity Proofing</td>
</tr>
</tbody>
</table>

## Standards and Specifications
- RSA PKCS#1 v2.1: RSA Encryption Standard
- RSA PKCS#7 v1.5: Cryptographic Message Syntax Standard
- RSA PKCS#10 v1.7: Certification Request Syntax Standard
- RFC 2630: Cryptographic Message Syntax (CMS)
- RFC 5126: CMS Advanced Electronic Signatures (CAdES)
- ETSI TR 119 312 Electronic Signatures and Infrastructures (ESI), Cryptographic Suites
- ISO29115 - 2013: Entity authentication assurance framework
- Regulation (EU) N°910/2014 – eIDAS
- ICAO passport
ABOUT GEMALTO

Gemalto is the world leader in digital security with 2017 revenues of €3 billion. In the civil identity sector, Gemalto provides secure documents, robust identity solutions and services that address government programs for ID management and road safety, trusted digital and mobile ID schemes and infrastructures for secure public eServices, and border and visa management requirements. Gemalto also addresses public safety and law enforcement challenges, offering best-in-class forensic solutions.

The company’s products and solutions are deployed in over 200 active programs worldwide, with specific expertise in secure document issuance, biometrics, document readers, authentication, ID management and data protection. Gemalto collaborates with its clients to report and share best practices.