



CRYPTOMATHIC SECURE MOBILE APPLICATION FOR SMART PHONES

Dynamic Two-Factor Authentication

The use of strong two-factor authentication (2FA) is now widely accepted as an insurance against attacks, such as phishing, pharming, trojans and man-in-the-middle, and to maintain customer trust. Yet, most organisations are struggling to achieve this level of security with authentication methods that mutually provide ease of use, scalability and cost efficiency. From small to large-scale deployments, key success factors also rely on the ease of implementation of current and future 2FA solutions.

The wide-spread use of mobile phones and the ubiquity of this technology can now be used, regardless of network coverage, for generating dynamic or one-time-passwords (OTPs), to offer organisations cost effective and easy-to-deploy two-factor authentication technology. This provides users with a strong, truly mobile and easy-to-use authentication channel to access enterprise, eGovernment or online banking applications.

Cryptomathic Mobile AuthApp

To complement its robust offering in strong authentication and electronic signatures, Cryptomathic has designed a user-friendly smart phone application that generates dynamic passwords on a large range of devices. The Cryptomathic Mobile AuthApp is based upon open standards such as OATH's event-based (HOTP), time-based (TOTP),



challenge response (OCRA) or MasterCard CAP / VISA DPA type implementations. Mobile AuthApp enables users to generate OTPs, allowing organisations to immediately verify user credentials, regardless of the user's location. Additionally, critical transaction data can be signed using Mobile AuthApp, thereby ensuring transaction integrity and defeating man-in-the-middle attacks.

Smart phone users are now accustomed to downloading apps and it seems natural to use them for strong authentication purposes. With no additional hardware required, this tokenless solution is easy to deploy, truly mobile and highly cost effective compared with legacy tokens. In addition, Cryptomathic Mobile AuthApp implements many other security features, including PIN protection and secure enrollment.

Mobile AuthApp can be optionally configured to follow specific workflows (e.g. for registration or re-initialization) or to follow a custom security policy. The ability to develop additional security features and functions without a full-blown re-deployment also makes Mobile AuthApp a current and future-proof 2FA solution. Comprehensive configuration capabilities provide a high level of customisation, e.g. the level of security needed or a custom logo to reinforce your branding, at no additional cost.

Organisations can distribute Mobile AuthApp on a relevant application server/store, allowing end-users to securely download and register their device within seconds. The deployment of 2FA tokens has, therefore, never been easier, as the generation and distribution of the Mobile AuthApp tokens can now be reduced to a single step for the organisation.

Once the application is installed, it does not require any data connection and hence no signal reception. It can therefore be used without incurring any transaction costs as opposed to OTPs sent via SMS.

In short, Cryptomathic Mobile AuthApp is a well-balanced 2FA solution between consumers' desire for usability and the organisation's need for cost-efficiency.

USABILITY

Discreet and
efficient

Truly mobile with
no running costs

Installed within
seconds

COST-EFFICIENCY

Reinforce customer
confidence and branding

Effective
against fraud

Seamless deployment
with reduced
overall investment

APPLICATION SPECIFICATIONS

On-Board Security Algorithm

- OATH Compliant Time-Based with choice of time step (T-OTP / RFC 6238)
- OATH Compliant Event-Based (H-OTP / RFC 4226)
- OATH Compliant Challenge Response Algorithm (OCRA / pending RFC 6287)
- MasterCard CAP & VISA DPA modes available

OTP Generation mode

- Upon application start-up
- (option) PIN/Password Protected

Key Storage for OTP Security Algorithm

- Protected with Device ID (IMEI) and User ID (Serial Number) and stored in the device memory.
- Re-registration process available any time

Operating systems

- Apple iOS
- Android
- Blackberry

T-OTP Time Source and synchronisation

- Time source: device local clock in UTC format
- A time acceptance window is to be configured on the server side
- Time drift adjustment is done on the server side during OTP validation process

Customization Available

- Custom Branding available
- Optional custom workflow based on "Cryptomathic core API"
- Optional multi-lingual support

Registration Process

- Application downloaded from relevant application server/store
- Registration can be initiated from either client or server, subject to preference

Back end server

- Any OATH compliant back-end can be used to validate OTPs
- Authentication method and registration processes readily supported with Cryptomathic Authenticator 3.6 / Signer

CRYPTOMATHIC AUTHENTICATOR

Authentication Mechanism Independent

The Authenticator is a one-stop 2FA solution which provides the highest level of flexibility and vendor independency to ensure organisations are able to quickly adapt to address new security threats and authentication requirements. In addition to providing a complete authentication package consisting of server software, hardware security modules (HSMs), installation, training and maintenance & support, the Authenticator readily supports a vast array of authentication methods.

The wide range of integrated authentication mechanisms includes MasterCard CAP / VISA DPA, OTP tokens (including Mobile AuthApp), SMS, PKI, Grid Cards, TAN lists, as well as more traditional static passwords, PINs and partial passwords. This enables full support of new token types and algorithms, with no impact on the existing infrastructure, token functionality and interfaces.

Through a flexible, highly scalable and best-practice approach, all Cryptomathic's solutions provide future-proof adaptability to meet the organisations' evolving requirements, thereby safeguarding the value of the initial investment.



ABOUT CRYPTOMATHIC

Cryptomathic is one of the world's leading providers of security solutions to businesses across a wide range of industry sectors, including finance, smart card, digital rights management and government. With more than 25 years' experience, Cryptomathic provides customers with systems for e-banking, PKI initiatives, card personalization, ePassport, card issuing

and advanced key management utilizing best-of-breed security software and services. Cryptomathic prides itself on its strong technical expertise and unique market knowledge. Together with an established network of partners, Cryptomathic assists companies around the world with building security from requirement specification to implementation and delivery.

Learn more at cryptomathic.com