CRYPTSOFT

FOUNDATION SECURITY TECHNOLOGIES
TRUSTED² | EMBEDDED | INTEROPERABLE

OTP Authentication Tokens

Wirelessly programmable OTP tokens

0101010110010010110100110111001010101101010101010

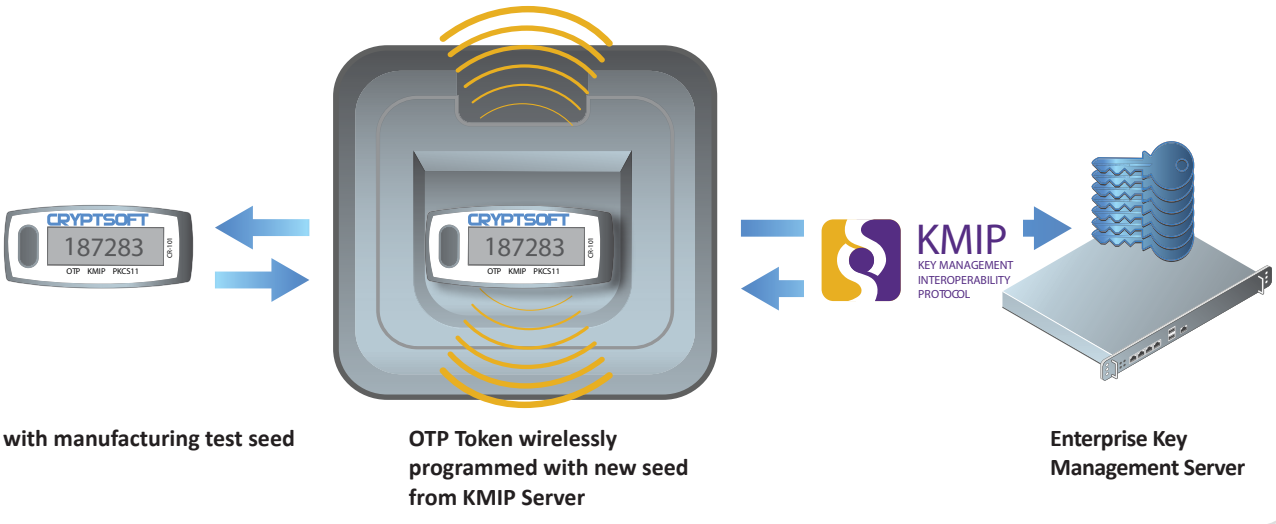
AUTHENTICATION

Cryptsoft and Feitian have collaborated to deliver a wirelessly programmable One-Time-Password (OTP) authentication token that is supported by Cryptsoft's OASIS Key Management Interoperability Protocol (KMIP) products.

Cryptsoft's OTP solution is based on open standards and allows the enterprise to manage the full lifecycle of the seed records that underpin the security in an OTP solution. This ensures that only the enterprise has access to the seed records, and the enterprise has full control over the provisioning, usage, and de-provisioning of tokens.

Key Features

- Strong two-factor authenticator
  - Unique password generated each time
- OATH compliant time-based TOTP device
  - Easy to integrate with third party systems
- Single-button OTP hardware token
  - 6 or 8 character LCD
- OASIS KMIP integration
  - Client authentication and seed provisioning



OTP with manufacturing test seed

OTP Token wirelessly programmed with new seed from KMIP Server

Enterprise Key Management Server

SALES@CRYPTSOFT.COM +61 7 3103 0321 | US +1 650 918 4362 **WWW.CRYPTSOFT.COM**

OTP Authentication Tokens

Wirelessly programmable OTP tokens

0101010110010010110100110111001010101101010101010

Time based One Time Password (TOTP) tokens provide users with a secure and reliable hardware device to integrate standards-based hardware two-factor authentication.

Two-factor authentication with TOTP combines something you know (your password) with something you have (a unique number sequence generated by a hardware device). Both of these factors are required to authenticate – substantially improving the security properties when compared to a single factor authentication solution.

The non-predictable six or eight digit token output is derived from both the secret seed record and the on-board real time clock (RTC).
A single hardware token can be programmed for variable output (6 or 8 digits) and variable time intervals (30 or 60 seconds) ensuring a solution is easily tailored to your enterprise security context.

Two (or more) tokens initialised with the same seed value can be used for person-to-person two-factor authentication entirely independent of any server infrastructure.

The same seed record can also be loaded into software based TOTP solutions allowing for a mixed hardware and software deployment context.

As tokens are now substantially more cost effective than in the past, each user can be issued with multiple tokens and replacement tokens in the case of token loss, enabling broader use of two-factor authentication within your enterprise.

• Algorithm	-	OATH TOTP
• Algorithm Class	-	Time-based
• Hardware Input	-	Built-in button
• Hardware Display	-	6-8 Character LCD
• Hardware Serial	-	Unique S/N
• Hardware Certificate	-	ROHS Compliant
• Operating Temperature	-	-10°C to 50°C
• Storage Temperature	-	-20°C to 70°C
• Casing	-	Hard molded ABS
• Physical Security	-	Tamper Evident
• Key Storage	-	Static RAM
• Data Retention	-	Lithium battery
• Battery Lifecycle	-	3-5 years
• Endurance	-	> 14,000 clicks
• Humidity	-	5% to 90%

SALES@CRYPTSOFT.COM +61 7 3103 0321 | US +1 650 918 4362 **WWW.CRYPTSOFT.COM**

@CRYPTSOFT @CRYPTSOFT CRYPTSOFT-SECURITY-SPECIALISTS