FORWARD THINKING IT SOLUTIONS

# ERGONOMICS AUTHENTICATION SERVER (EAS)

## Server for EMV-CAP, OATH, Digipass and CrontoSign Multifactor Authentication for Electronic and Mobile Banking Applications

### Easy Integration of EMV-CAP, OATH, Digipass, mTAN or CrontoSign Technology in Existing Backend Systems

EMV-CAP is the international standard for strong authentication for e-banking and e-commerce. OATH and Digipass are well established standards for one-time password solutions. CrontoSign is an innovative technology for authentication and transaction verification based on 2D bar codes.

CAP (Chip Authentication Program) was developed by MasterCard and adopted by Visa (Visa Passcode) to secure Internet-based e-commerce transactions with debit- and credit cards. The CAP standard supports strong authentication also for e-banking applications.

### Required Components for EMV-CAP

To integrate EMV-CAP, a financial institution requires the following components:

- EMV debit-, credit- and/or bank cards, appropriately personalized
- Personal Card Reader (PCR) for the customers
- EMV-CAP Authentication Server for the verification of one-time passwords and transaction signatures

Ergonomics offers e.g. OneSpan/Vasco Personal Card Readers (PCRs) and the Authentication Server for easy and efficient integration of EMV-CAP into existing backed systems.

### OTP Token and SMS Delivery, Cronto Sign

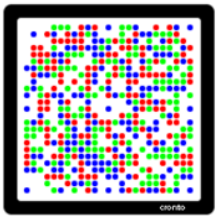
Feitian one-time password tokens (OATH algorithm) or OneSpan/Vasco Digipass tokens can be used in scenarios where a cost efficient but highly secure multifactor authentication solution is required.

SMS delivery of one-time passwords and transaction signatures as well as EMV-CAP card readers are supported. In addition, the EAS supports the sophisticated 2D color bar code technology CrontoSign by OneSpan/Vasco for authentication and transaction verification.

ergonomics

# ERGONOMICS AUTHENTICATION SERVER (EAS)

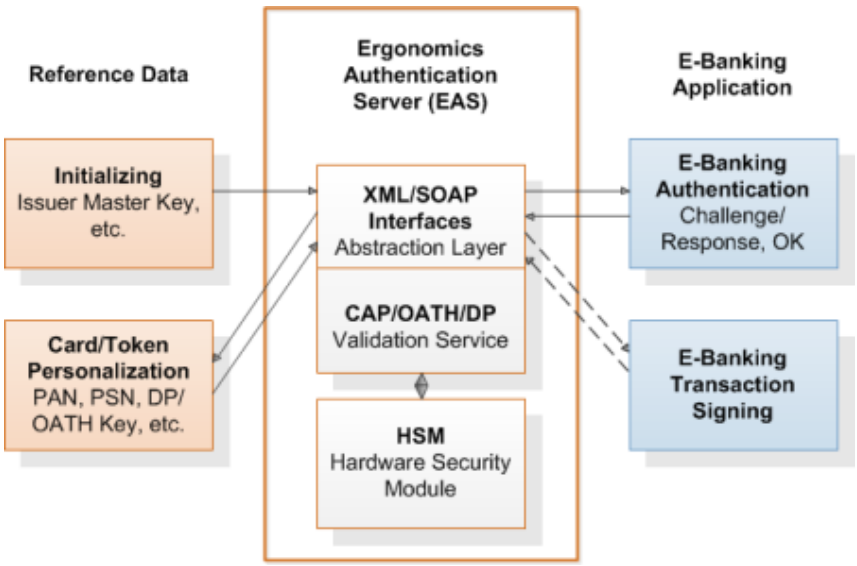
## EAS Key Functionalities



The Ergonomics Authentication Server provides the following key features:

- Initialization and key management
- Data preparation for the card personalization
- Protected data import for OATH, Digipass and CrontoSign keys
- Interface to SMS gateways to send one-time passwords and transaction verification data
- Verification of one-time passwords at application log-on
- Verification of transaction signatures
- Support for behavior-based authentication (continuous authentication) for mobile and e-banking.

The following illustration provides an overview of the typical system environment of the Ergonomics Authentication Server.




## Easy Integration

The easy integration of the EAS into existing banking infrastructures was one of the primary design goals. Web Services Interfaces provide the necessary flexibility for the integration.

A typical bank has already some e-banking services in place today but may lack adequate user authentication and/or transaction verification technology. Therefore, the EAS works for example in combination with existing user directories and conventional authentication methods, based on user name and password.

Depending on the existing environment and the requirements of the bank, only a subset of the capabilities can be implemented. For example: a bank may only need transaction verification. The current user authentication is considered sufficient. The modular design of the EAS can easily accommodate this requirement.

## Hardware Security Modules (HSMs) for a higher level of Security

The EAS supports HSMs for the protection of the sensitive encryption keys. This allows bank to achieve the highest level of security available today. In addition, HSMs may be required to achieve necessary compliance levels.

## More Information

Please contact us for more information about the EAS: sales@ergonomics.ch

1AA

Ergonomics AG » Uetlibergstrasse 132 » CH-8045 Zürich
info@ergonomics.ch » www.ergonomics.ch
+41 58 311 10 00