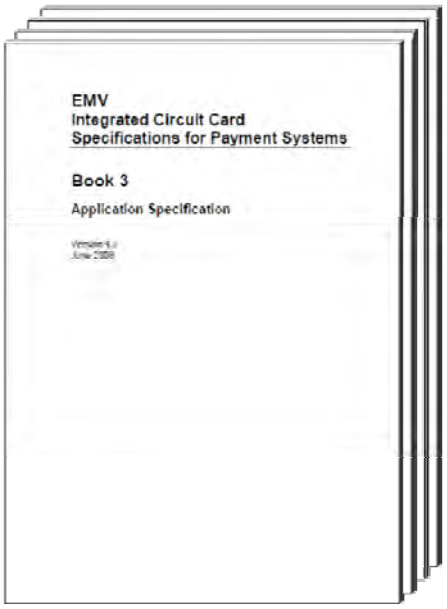
Extending EMV payment smart cards with biometric on-card verification

Olaf Henniger and Dimitar Nikolov
Fraunhofer IGD
Fraunhoferstrasse 5
64283 Darmstadt

What are EMV cards?

- Debit and credit cards with a microprocessor chip (smart cards)
- Complying with the EMV specifications, the common-ground standard for smart-card based payment systems
- Based on ISO/IEC 7816
- Named after Europay, MasterCard, and Visa, who created the first version of the spec in the 1990s
- Being introduced worldwide because, unlike a magnetic stripe, the chip cannot be cloned



How do EMV transactions work?

- Application selection
- Initiate application processing and read application data
- Offline data authentication using public-key cryptography
- Processing restrictions
- Cardholder verification
- Terminal risk management
- Terminal action analysis
- Card action analysis
  - Transaction certificate (TC): Offline approval
  - Application authentication cryptogram (AAC): Offline decline
  - Authorisation request cryptogram (ARQC): Go online
- Conditionally online processing
- Completion and script processing

Cardholder verification

- Card issuer defines cardholder verification (CV) rules list specifying which CVM to apply
  - Offline PIN
  - Online PIN
  - Handwritten signature on paper

  under what conditions
  - Always;
  - Terminal supports CVM;
  - Transaction is in the application currency and is under/above a value X.
- The terminal processes the CV rules list until
  - A CVM is performed successfully;
  - A mandatory CVM failed;
  - The list is exhausted.

Proposed extensions for biometric cardholder verification

- Define a new CVM for each biometric on-card verification method
- Extend the definitions of the commands used for PIN verification to support biometric on-card verification
- Extend the data elements terminal verification result (TVR), terminal action code (TAC), and issuer action code (IAC) to hold information about biometric cardholder verification
- Add the data elements on the card
  - Biometric information template (BIT): For informing the terminal about properties of the biometric cardholder verification method [ISO/IEC 7816-11].
  - Biometric reference, and
  - Biometric retry counter

Biometric cardholder verification

- Retrieve the BIT
- If the biometric CVM is supported and not blocked,
  - Capture biometric data,
  - Format them according to the BIT,
  - Send them to the card for on-card comparison

Prototype

- Uses Java-card applet for handwritten signature on-card verification
- Comparison of signature dynamics (time series of x and y coordinates) using dynamic time warping (DTW) algorithm

Is handwritten signature on-card verification secure?

- More secure than handwritten signature on paper
- Security depends on quality of the enrolment template – Biometric sample quality assessment at enrolment time is crucial.
- In case of false accepts
  - Chargeback if the customer denies the payment (like for handwritten signature on paper)
- In case of false rejects
  - The card should still offer PIN verification.

Summary and outlook

- MSc project showed feasibility of extending EMV cards with biometric on-card verification
- We argue that handwritten signature on-card verification would be
  - User-friendly,
  - Secure, and
  - Privacy-preserving
- Things to do before a market launch:
  - Amending the EMV specifications
  - Porting from Java card to native-code smart cards in order to reduce computing time
  - Integration of signature pad into point-of-sale terminals
  - Security evaluation

Confirm the amount

Insert the card

Fraunhofer IGD

Sign your name

Fraunhofer IGD

Payment authorised by card

Fraunhofer IGD

Fraunhofer
IGD

Dr. Olaf Henniger

Deputy Head of Competence Center
Identification and Biometrics
Fraunhofer Institute for Computer Graphics Research IGD

Fraunhoferstrasse 5 · 64283 Darmstadt · Germany
Phone +49 6151 155-526 · Fax -499
olaf.henniger@igd.fraunhofer.de