FINEID - S1

Electronic ID Application

v4.0

Population Register Centre (VRK)
Certification Authority Services
P.O. Box 123
FIN-00531 Helsinki
Finland
http://www.fineid.fi

Authors

Name	Initials	Organization	E-mail
Jari Pirinen	JP	VRK	jari.pirinen@vrk.fi

Document history

Version	Date	Editor	Changes	Status
0.1	17.05.2019		Initial version.	Initial version.
1.0	29.05.2019	JP	Document accepted.	Published version.

Table of contents

1. Introduction 3
1.1 Normative and informative references 3
1.2 Related FINEID documentation 3
2. Functionalities implemented outside the scope of Gixel IAS ECC 4
2.1 Secure Messaging and PACE 4
2.2 Elliptic Curve Cryptography (ECC) 4

1. Introduction

This document describes the implementation of VRK (PRC) Organisational Cards with the following ATRs:

Contact ATR	#3BDD96008031FE450031B8640429ECC1739401808248
Contactless ATR	#3B898001805743495A323191

1.1 Normative and informative references

The implementation of VRK (PRC) Organisational Cards is based on *Gixel IAS ECC, Identification Authentication Signature European Citizen Card, Technical Specifications, Revision: 1.0.1.*

The functionalities that have been implemented outside the scope of the above specification are:

- Secure Messaging and PACE.
- Elliptic Curve Cryptography (ECC).

For additional information on the above functionalities, refer to:

- *ICAO (International Civil Aviation Organization) Doc 9303, Machine Readable Travel Documents, Seventh Edition 2015, Part 11: Security Mechanisms for MRTDs.*
- *Idemia Organizational Cards - S1, Electronic ID Application, Issue Date 2019-02-15.*

1.2 Related FINEID documentation

Related FINEID documentation is available from: https://vrk.fi/fineid-maaritykset.

2. Functionalities implemented outside the scope of Gixel IAS ECC

2.1 Secure Messaging and PACE

Secure Messaging and PACE have been implemented according to ICAO (*International Civil Aviation Organization) Doc 9303, Machine Readable Travel Document, Seventh Edition 2015, Part 11: Security Mechanisms for MRTDs*.

The exception to the above specification is, that instead of MRZ and CAN authentication, the user is authenticated using PIN1 and PIN2.

2.2 Elliptic Curve Cryptography (ECC)

Elliptic curve cryptography has been implemented according to *Idemia Organizational Cards - S1, Electronic ID Application, Issue Date 2019-02-15.*