# ISO/IEC 25791-1:2026-09 (E)

## Information technology - OpenID Connect FAPI Security Profile 1.0 - Part 1: Baseline

## Contents

Page


Foreword ..... iv

Introduction ..... v

Notational conventions ..... vi

1. Scope ..... 1

2. Normative references ..... 1

3. Terms and definitions ..... 2

4. Symbols and abbreviated terms ..... 2

5. Baseline security profile ..... 2
5.1 Introduction ..... 2
5.2 Baseline security provisions ..... 3
5.2.1 Introduction ..... 3
5.2.2 Authorization server ..... 3
5.2.3 Public client ..... 5
5.2.4 Confidential client ..... 5

6. Accessing Protected Resources ..... 6
6.1 Introduction ..... 6
6.2 Baseline access provisions ..... 6
6.2.1 Protected resources provisions ..... 6
6.2.2 Client provisions ..... 7

7. Security considerations ..... 7
7.1 TLS and DNSSEC considerations ..... 7
7.2 Message source authentication failure ..... 7
7.3 Message integrity protection failure ..... 8
7.4 Message containment failure ..... 8
7.4.1 Authorization request and response ..... 8
7.4.2 Token request and response ..... 8
7.4.3 Resource request and response ..... 8
7.5 Native Apps ..... 8
7.6 Incomplete or incorrect implementations of the specifications ..... 9
7.7 Discovery & Multiple Brands ..... 9

8. Privacy considerations ..... 9

Annex A (Informative) Acknowledgement ..... 11

Notices ..... 12

Bibliography ..... 13