

IN GROUPE DENMARK PS

Authentication and Credential Management Practice Statement

Document information			
No of pages: 10	Reference: N/A	Department: eID Application Development	Classification: Public
Valid from: 11/08/2026		Last saved update: 28/08/2026	Version: 1.2



Authentication and Credential Management Practice Statement

Reference: N/A

Version: 1.2

Creation Date:11/08/2026

Latest updated:28/08/2026

TABLE OF CONTENTS

Table of Content	2
Version Control and Revision History	3
References	3
Introduction	4
1 Applicable definitions	4
2 Technical specifications and procedures	5
2.1 Enrolment	5
2.1.1 Application and Registration	5
2.1.2 Identity Proofing and Verification (Natural Person)	6
2.1.3 Identity Proofing and Verification (Legal Person)	6
2.1.4 Binding between the electronic identification means of natural and legal persons	6
2.2 Electronic identification means management	6
2.2.1 Electronic identification means characteristics and design	6
2.2.2 Issuance, delivery and activation	7
2.2.3 Suspension, revocation and reactivation	7
2.2.4 Renewal and replacement	8
2.3 Authentication	8
2.3.1 Authentication mechanism	8
2.4 Management and organisation	9
2.4.1 General provisions	9
2.4.2 Published notices and user information	9
2.4.3 Information security management	9
2.4.4 Record keeping	9
2.4.5 Facilities and staff	9
2.4.6 Technical controls	9
2.4.7 Compliance and audit	10

	Authentication and Credential Management Practice Statement	Reference: N/A
		Version: 1.2
		Creation Date:11/08/2026
		Latest updated:28/08/2026

VERSION CONTROL AND REVISION HISTORY

Version Number	Date of Change	Author/Modifier	Summary of Changes
1.0	22-05-2025	Robert Peter Laursen	First version
1.1	27-06-2025	Robert Peter Laursen	Update after conformity assessment stage 1 review
1.2	14-08-2026	Carl Pedersen	Added support bank-based onboarding, clarified the use of email as a unique identity identifier, added relying-party-specific identifiers and CIBA authentication and updated authenticator management and revocation procedures.

REFERENCES

ID	Version	Description
[1]	1.1	Trust Service Practice Statement
[2]	1.2	Identity Proofing Practice Statement
[3]	n/a	EU Commission Implementing Regulation 2015/1502
[4]	2.1.1	ETSI TS 119 461 V2.1.1 (2025-02), Annex C.3.4 – Use case for identity proofing by other identification means



Authentication and Credential Management Practice Statement

Reference: N/A

Version: 1.2

Creation Date:11/08/2026

Latest updated:28/08/2026

INTRODUCTION

IN Groupe Denmark A/S is the provider of the white-label Identity provider platform called "IN ID" and used by trust service providers for identity proofing, authentication, and credential management. The identity proofing component used by IN ID is called "IN ID Verify" and is also provided as a standalone product.

The IN ID practice statement documentation is organised as described below:

- "Authentication and Credential Management Practice Statement" describes how requirements from EU Implementation reference 2015/1502 are met (current document) for "IN ID".
- "Trust Service Practice Statement" [1] describing how the general requirements from eIDAS and ETSI EN 319 401 are met for "IN ID".
- "Identity Proofing Practice Statement" describing how the requirements from ETSI TS 119 461 are met for "IN ID Verify".

1 APPLICABLE DEFINITIONS

Term/Acronym	Definition
Applicant	An individual or entity undergoing an identity proofing and enrolment process to become a Subscriber. Also referred to as the end-user.
Authentication	The process of establishing the identity of an end-user and answers the question "Prove you are who you say you are."
Authenticator	Something the end-user possesses and controls (e.g., a cryptographic key, a password, an OTP device) that is used to authenticate their identity.
Biometrics	Measurable physical characteristics (e.g., fingerprint, facial features) or behavioural traits used for identity verification or authentication.
CSP	Credential Service Provider: An entity responsible for identity proofing individuals and issuing and managing their authenticators. In the context of this document, IN Groupe acts as a CSP for the defined services.
eIDAS	Electronic Identification, Authentication and Trust Services: EU Regulation 910/2014.
End-user	Synonym for subscriber or applicant.
ETSI	The European Telecommunications Standards Institute (ETSI).
FAL	Federation Assurance Level: A measure of the assertion strength in a federated identity environment, as defined in NIST SP 800-63C.
IAL	Identity Assurance Level: A measure of the confidence in a claimed identity following an identity proofing process, as defined in NIST SP 800-63A.
Identification	The process of claiming an identity, typically through a username or other identifier. It answers the question "Who are you?".
Identity Proofing	The process of confirming that an individual is who they claim to be, typically involving the validation of identity evidence. Ref. [2]
IdP	Identity Provider: A system that manages and verifies digital identities.
IN ID	The IN Groupe identity platform.
LoA	Level of Assurance refers to the degree of confidence in the claimed identity of an individual in an authentication. LoA is a function of the IAL, FAL and the strength of the authenticator(s) used in the authentication.
MFA	Multi-Factor Authentication: An authentication method that requires the end-user to provide two or more verification factors from different categories (something you know, something you have, something you are).
OIDC	OpenID Connect, a modern, standardised way for applications (RP) to verify who an end-user is and get basic profile information about them



Authentication and Credential Management Practice Statement

Reference: N/A

Version: 1.2

Creation Date:11/08/2026

Latest updated:28/08/2026

PIN	Personal Identification Number
Relying Party (RP)	An entity that relies upon a Subscriber's authenticated identity and related attributes, as asserted by the CSP.
Scope	OIDC scope defines the eID attributes set that a client (an RP application) requests to obtain about a user's identity from an Identity Provider (IdP). A scope could be knowing if the subscriber is above or below a certain age.
Subscriber	An individual or entity that has successfully completed the IDV and enrolment process and has been issued authenticators by the CSP. Also referred to as the end-user

2 TECHNICAL SPECIFICATIONS AND PROCEDURES

2.1 Enrolment

2.1.1 Application and Registration

The application and registration processes are initiated and completed by the end-user through the IN ID mobile application. Identity proofing and verification may be performed using one of the supported identity proofing methods described in [2] using IN ID Verify, or through other supported onboarding methods, such as eID federation or bank onboarding, as applicable.

The first step in the mobile application and registration flows for the end-user is:

- The end-user is presented with a link to the current Terms and Conditions that he can read, download and/or print. An end-user security guide (in the section 'User Obligations') is part of the terms and conditions.
- The end-user is presented with a link to the current Privacy Policy that the end-user can read, download and/or print.
- The end-user must actively accept the Terms and Conditions and the Privacy Policy by checking a checkbox. The registration process cannot continue until this checkbox has been checked.
- The end-user acceptance of the Terms and Conditions and Privacy Policy is logged, including the version number of the Terms and Conditions, in the audit log in the IN ID backend.

As part of the registration process, a valid email address is required for the identity. The email address is validated and must be unique within IN ID. An email address already associated with an existing identity cannot be associated with another identity.

The IN ID mobile application is designed so that the end-user cannot use the app, if the app version is marked as suspended in the IN ID backend.

In case a new version of Terms and Conditions is released, the mobile app cannot be used until the end-user accepts this latest version of the Terms and Conditions.

The system automates the collection of data required for identity proofing and verification. Depending on the applicable onboarding method, the data may be obtained from an identity document, a notified eID scheme,



Authentication and Credential Management Practice Statement

Reference: N/A

Version: 1.2

Creation Date:11/08/2026

Latest updated:28/08/2026

or a customer-specific bank-based onboarding process, in accordance with the methods described in 2015/1502 section 2.1.2.

Types of data collected, as part of the identity proofing, are designed to comply with data minimisation principles and GDPR. The actual data collected is described in “Identity Proofing Practice Statement” [2].

2.1.2 Identity Proofing and Verification (Natural Person)

Ref. to “Identity Proofing Practice Statement” [2].

The system automates the collection of data required for identity proofing and verification. Depending on the applicable onboarding method, the data may be obtained from an identity document, a notified eID scheme, or a customer-specific bank-based onboarding process, in accordance with the methods described in 2015/1502 section 2.1.2.

2.1.3 Identity Proofing and Verification (Legal Person)

Legal persons are not supported.

2.1.4 Binding between the electronic identification means of natural and legal persons

Legal persons are not supported.

2.2 Electronic identification means management

2.2.1 Electronic identification means characteristics and design

The IN ID platform provides applicants with a secure and user-friendly app for both iOS and Android. The app is a mobile application that integrates the IN ID SDKs for the control of identity proofing, enrolment, activation, authentication, and lifecycle management.

No personal data is stored on the device; only the necessary keys to link the app instance to the data stored in the backend system are kept locally.

The app provides strong multi-factor authentication (MFA) by utilizing a knowledge factor (the PIN) in conjunction with a possession factor (two private keys).

At assurance level substantial, the subscribers have the option to unlock the app using biometrics instead of the PIN. However, the PIN will always serve as a backup, ensuring access in case biometric recognition fails (e.g., due to wet fingers).



Authentication and Credential Management Practice Statement

Reference: N/A

Version: 1.2

Creation Date:11/08/2026

Latest updated:28/08/2026

When biometric recognition is enabled as an alternative to manually entering the app PIN, the PIN is protected by an encryption key linked to the device's biometric authentication mechanism.

When disabling biometric recognition for unlocking, the PIN and any derived values are immediately zeroed out and cleared from the device's memory after each use, whether the PIN is entered directly or unlocked via biometric recognition.

For app enrolment on authenticator assurance level high, the use of biometric recognition is not allowed.

2.2.2 Issuance, delivery and activation

The app must be downloaded from the official App Store or Google Play, to start and complete the activation.

The end-user must, as part of the app activation process, accept the current Terms and Conditions and the Privacy Policy before the identity proofing can be initialised.

To ensure that the app is logically bound to a specific end-user, a unique activation code is issued and handled electronically i.e. generated and transferred directly to the app without the end-user needing to input it. The activation code is issued when the end-user has successfully completed one of the identity proofing and verification flows, as described in [2].

The authenticator assurance level assigned to the app may be equal to or lower than the identity assurance level achieved through the identity proofing and verification process, depending on the authentication use cases supported by the app.

When the above activation is validated, the end-user must create their own personal 6 digit app PIN. This PIN is centrally validated, providing strong protection against online guessing attacks.

During app activation, two private keys are generated on the device and stored securely on the device. The corresponding public keys are registered in the app backend, enabling secure communication between the app and the backend and allowing for integrity of app-signed transactions to be verified.

2.2.3 Suspension, revocation and reactivation

If the end-user enters the wrong PIN more than 3 times, the app authenticator is temporarily suspended and later automatically reactivated, after a predefined period (suspension period is configurable).

In case the end-user has forgotten the app PIN, the end-user will need to delete the app, and use the account recovery flow in the mobile app. The flow will revoke the previous app instance and activate a new app instance. Similarly, if the end-user loses his phone, and enrolls a new device, the authenticator associated with the previous app instance is automatically revoked.

The app, and optionally the eID, can also be revoked by the end-user in the activated app. The revocation requires physical possession of the device and knowledge of the app PIN (or biometric) to revoke the eID. Should an end-user need to urgently revoke their app, for example due to loss of possession of the device, a secure web portal is available for this purpose. Alternatively, a trusted support function, operating under strict security protocols and access controls, can revoke the app on behalf of the end-user.

	Authentication and Credential Management Practice Statement	Reference: N/A
		Version: 1.2
		Creation Date:11/08/2026
		Latest updated:28/08/2026

Reactivation of a revoked app is not possible. As mentioned, the end-user (the natural person) can follow the app activation flow to activate a new app instance.

2.2.4 Renewal and replacement

Centralised policy controls are implemented to ensure the apps operate exclusively within a secure and compliant environment. These policies enable the suspension of apps installed on devices operating with outdated operating system versions, specific device models, or prior app versions. End-users are subsequently prompted to update (replace) to the latest app version available from the official App Store or Google Play.

This proactive and policy-driven update mechanism, together with the robust security architecture of the app (detailed in sections 2.2.1 and 2.2.2), guarantees the continuous integrity and trustworthiness of the app. This continuous security removes the necessity for a traditional application renewal process; the app remains active until revoked.

2.3 Authentication

2.3.1 Authentication mechanism

Authentication is performed in accordance with the standard OpenID Connect using either the Authorization Code Flow or the Client Initiated Backchannel Authentication (CIBA) Flow. Upon successful authentication, a cryptographically signed ID token is issued to the relying party.

To reduce the risk of cross-service correlation and tracking, IN ID uses relying-party-specific identifiers. The internal unique identifier of an identity is not disclosed to relying parties. Instead, each relying party is provided with a unique and stable identifier that is internally mapped to the corresponding identity. Different relying parties therefore receive different identifiers for the same identity, preventing correlation across relying parties based on the identifier.

The relying party can provide a “reference text”, which is displayed in both the web-client and the app as part of the authentication request. The reference text provides the end-user with contextual information that enables them to recognise and verify that the authentication request originates from an expected source. If no custom reference text is provided, a specific session text is displayed in the app. A relying party specifies a LoA, when initializing an authentication and requests personal attributes (via the requested scope) to be included in the signed response.

The binding of the app to the authentication request at the relying party is obtained via a session QR code or through app switch. When scanning the QR code, the app instance, and hence the end-user, is linked to the authentication request. When the authentication request is initiated from an app published by the relying party, or in a mobile browser, the binding is established via an app switch mechanism.

The end-user approves or rejects the authentication by:

1. The end-user scans the QR code or opens the app through app switch feature.



Authentication and Credential Management Practice Statement

Reference: N/A

Version: 1.2

Creation Date:11/08/2026

Latest updated:28/08/2026

2. The end-user enters the PIN or uses biometric recognition, if enabled.
3. The app displays the reference text and information identifying the relying party requesting authentication.
4. If the relying party has requested personal attributes, the app displays a consent prompt identifying the information to be shared.
5. The end-user swipes to approve the transaction or presses the relevant control to cancel it.

The signed authentication process is protected using TLS ensuring the confidentiality of the response during transit.

When the Terms and Conditions and/or the Privacy Policy are updated, the end-user is prompted to accept the newest version. The end-user will not be able to authenticate, until the newest version of Terms and Conditions and/or Privacy Policy are accepted.

2.4 Management and organisation

2.4.1 General provisions

See Trust Service Practice Statement [1].

2.4.2 Published notices and user information

See Trust Service Practice Statement [1].

2.4.3 Information security management

See Trust Service Practice Statement [1].

2.4.4 Record keeping

See Trust Service Practice Statement [1].

2.4.5 Facilities and staff

See Trust Service Practice Statement [1].

2.4.6 Technical controls

See Trust Service Practice Statement [1].

	Authentication and Credential Management Practice Statement	Reference: N/A
		Version: 1.2
		Creation Date:11/08/2026
		Latest updated:28/08/2026

2.4.7 Compliance and audit

See Trust Service Practice Statement [1].