iDIN Product sheet

For Merchants

Version 2.0

10-8-2018

This product sheet is intended for Merchants. The items it contains are 1) an explanation of the various parties in the process of using iDIN, 2) a flowchart clarifying the allocation of roles and the process, 3) information about the data that can be processed when using iDIN, 4) information about the reliability, security, privacy, and quality of the data when using iDIN, and 5) additional information about availability and storage periods, and other documentation.

Contents

1 The various roles

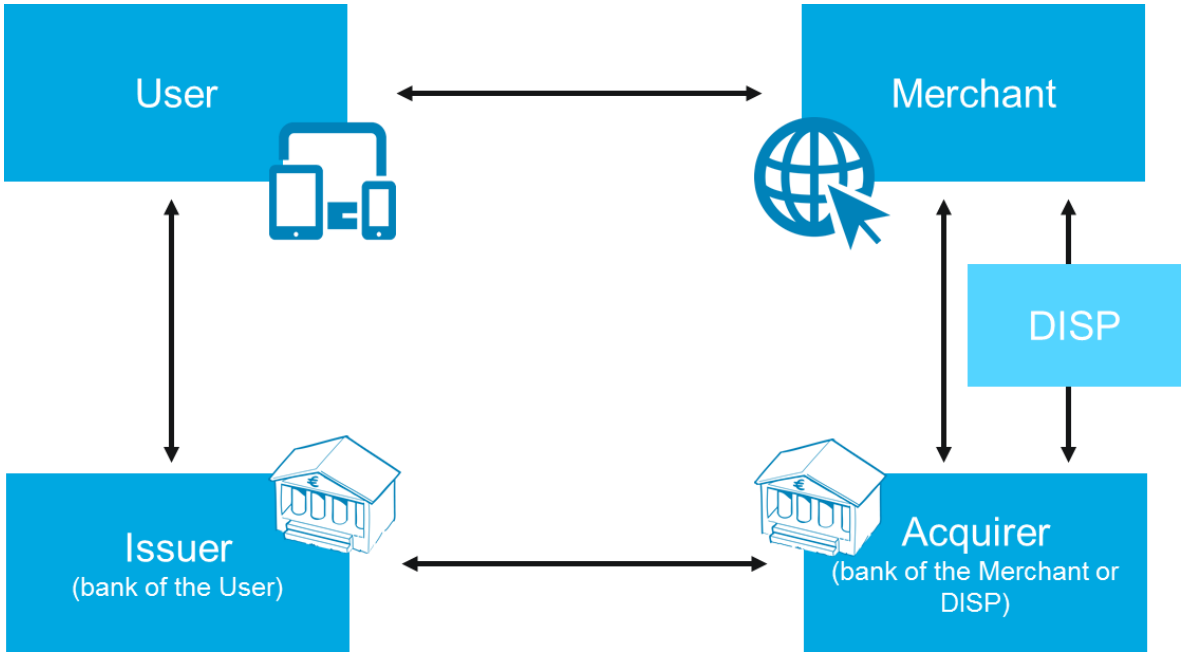
The various roles	
Role	**Explanation**
Merchant	A company/service/organisation that would like to use an easy and secure online identification method and give the User (customer) more choice when logging in, and is able to do so by offering iDIN as an extra online identification service on its website.
Acquirer	A party that has a Licence Agreement for iDIN with Currence (iDIN B.V.) and which concludes contracts with Merchants and DISPs for iDIN.
Data processor	A party that receives only encrypted or non-encrypted iDIN User data and then supplies it to the Merchant or only manages customer data on behalf of the Merchant. This party has no formal role within iDIN.
DISP - Digital Identity Service Provider	A party that has a Certificate Agreement for iDIN with Currence. The DISP makes agreements with its Merchants concerning iDIN and concludes iDIN contracts with its Merchants itself.
User	A natural person with access to the online channel of their Issuer provided with the correct authorisations. Their data are registered by their bank, the Issuer.
Issuer	A party that has a Licence Agreement with Currence. It is the User's consumer bank.

Role – General Data Protection Regulation (GDPR)	**Role iDIN**
Joint responsibilities - The legal persons that jointly determine the means for processing personal data within the framework of the iDIN system of agreements. For iDIN, the Issuer and Acquirer share joint responsibility for secure processing within the iDIN Scheme[1].	• Acquirer • Issuer
Responsible party - The legal person that determines the purpose for and means of processing personal data. The Merchant is therefore itself responsible for processing personal data of the IDIN service.	• Merchant
Processors - The party that processes personal data on behalf of the responsible party, without being subject to their direct authority. In accordance with the prevailing agreements of the iDIN scheme. For iDIN: • The RSP[2] is processor as defined by the GDPR for the Acquirer; • The VSP[3] is processor as defined by GDPR for the Issuer; • The DISP[4] is processor as defined by GDPR for the Merchant;	• Data processor • DISP
Party involved - The party to which the personal data to be processed relates. For iDIN, these are natural persons using iDIN services.	• User

[1] A Scheme is a system of functional, organisational, and technical agreements as described in further detail in the R&R Online for the iDEAL, iDIN and eMandates Products.
[2] A Routing Service Provider offers its services for the routing of a iDIN message, initiated by a User by means of the online channel of its Issuer through the website of the Merchant or DISP.
[3] A Validation Service Provider is responsible for processing iDIN messages on behalf of Issuers.
[4] A DISP with only a contractual relationship with the Merchant, where the technical processing of the IDIN messages therefore takes place directly between the Acquirer and the Merchant, should also be certified as a DISP; however, it does not have the role of processor.

2 iDIN Flowchart

The following flowchart has been made to show clearly how roles are allocated and to show the process of how iDIN is implemented and managed. The flowchart can best be viewed in combination with the table on the previous page.



3 What data can iDIN process?

iDIN provides various data that can be requested individually or as a combination.

Unique number for logging in

- BIN - Bank Identification Number, suitable for repeat log ins (number is allocated by the User's bank (Issuer) and gives the User a unique identity in their dealings with Merchants);
- Transient_ID for one-off use (one-off number allocated by the Issuer to the message in question).

Verified User data

Originating from an independent source, the legal identity document:

- Name: initial(s), prefixes, last name (legal last name)
- Age indication (18 years or older) or date of birth;
- Gender.

Data issued to the bank by the User

- User's preferred last name (preferred / partner last name)
- Residential address; street, house number, postcode, city/town;
- Email address;
- Telephone number.

Users have the option to not include the phone number and/or email address in the transaction, or to include a manually entered phone number and/or email address.

iDIN consists of several product types that can be used in different use cases:

- Identify
- Login
- Confirm age

4 Reliability, quality, privacy & security

4.1 Level of Assurance

When using electronic means of identification, it is important that they are reliable, secure, and of high quality. There are specific requirements that an Issuer's electronic means of identification must meet in order to be admitted to the iDIN Scheme. The requirements are based on the European eIDAS regulations and consist of technical specifications and procedures. Different requirements apply to each level, relating to registration, the management of electronic means of identification, authentication, management, and organisation. There are three different levels of assurance – low, substantial, and high. For iDIN, Issuers must in all cases offer an electronic means of identification to their Users that is at least compliant with level of assurance *substantial*. More information is available in the eIDAS regulations.

The main features of the level of assurance *substantial* are:

- Identification based on a valid identity document. The identity of the consumer should be verified using this valid identity document.
- Two-factor authentication is used (this means that you can only gain access with something you know (a password or code), together with something you have (a pass or token)).

4.2 Data quality

In order to ensure a high level of quality, iDIN has set requirements regarding the quality of data provided by Issuers, like format and content. Checks are made whether the data is present, whether it meets the required field format and if the data in the bank's database corresponds to the identity document.

The iDIN consumer target group meets the following conditions[5]:

- Natural persons;
- With access to the internet or mobile banking[6];
- Whose Money Laundering and Terrorist Financing (Prevention) Act (Wwft) compliance has been identified by the bank.

The criteria for measuring the quality assessment of data and the standards for the criteria are as follows:

Measurement criteria	Explanation	Standard
Accuracy	The extent to which iDIN data fields correspond to what is registered on the copy of the identity document.	95 – 99%
Completeness	The extent to which iDIN data is present: the data fields from the data model have been populated.	98 – 100%
Correctness	The extent to which iDIN data complies with the required field format: complies with the formatting rules as described in the most recent version of the iDIN Merchant Implementation Guidelines.	99%
Uniqueness	The extent to which iDIN data (in this case BSN) is unique: occurs only once with an Issuer.	97%

[5] Each bank is free to delimit this further. Business representatives, for example, are currently excluded.

[6] The banks apply the following minimum age limits for iDIN users: ABN AMRO, ASN Bank, RegioBank and SNS 18+; Rabobank and Triodos 16+; ING 12+.

4.3 Privacy & security

In the design of iDIN various measures have been taken in order to safeguard privacy and guarantee security:

- iDIN is based on the principle of privacy by design principle: privacy enhancing technologies and data minimization.
- The User instruct their bank to issue the information that is needed for them to be identified by an organisation.
- An organisation may store personal data provided by a bank, as long as the organisation observes privacy laws and uses the data solely for the purposes made known to the customer.
- Bank log-in details are entered by the User only in the internet environment of their own bank and not in that of online shops. This information remains known only to the customer.
- The User logs in to their own bank through a secure connection, out of sight of third parties;
- The User uses their own existing and secure bank methods to log in and to use iDIN.
- Data is sent encrypted to Merchants.
- A system of real-time online fraud detection has been set up in order to identify and combat any cases of fraud as early as possible.
- By using existing bank infrastructure, iDIN has the same high security, fraud-proofing and monitoring, such as the existing internet banking and iDEAL products.

5 Extra information

5.1 Availability

The overall period of availability is separated into two periods: prime time (06.00-00.30) and non-prime time (00.30-06.00). During prime time hours there should be online real-time availability of the systems for 99.5% of the time in each calendar month; for non-prime time hours this figure is 93.5%. The Acquirer or DISP should only carry out scheduled maintenance in the non-prime time period.

5.2 Storage period

Transaction details exchanged as part of the message protocols shall be retained for periods specified by law (in either electronic or physical archives or logs). The Acquirer is obliged to observe the retention periods stipulated in the iDX, or for a period of at least 13 months.

5.3 Additional information (www.idin.nl)

The following documentation can be requested on:
https://www.idin.nl/acceptanten/documentatie-aanvragen/

- Merchant Implementation guidelines
    - Including the annex diversity in consumer attributes - the Merchant should bear this in mind when integrating iDIN
- Software libraries (Java, .NET, PHP) and manual
- House Style Manual
- Toolkit organisations
- Background documentation
- Banners
- Logo

User demo: https://demo.idin.nl/
iDIN testimonials: https://www.idin.nl/acceptanten/acceptanten-aan-het-woord-video/
Animation: https://www.idin.nl/consumenten/animatie/animation/